Homogeneous Cyber Management of End-Points and OT

D7.1 Market Analysis and Market Impact Report

Deliverable type:	Document
Deliverable reference number:	ITEA 23022 | D7.1
Related Work Package:	WP 7
Due date:	May 2026
Actual submission date:	24 September 2026
Responsible organization:	3E
Editor:	Gofran Chowdhury
Dissemination level:	Public
Revision:	1.0

Abstract:	This deliverable establishes the market baseline for Work Package 7 of the HOMEPOT project. It characterises the global market for Mobile Device Management, Unified Endpoint Management, and adjacent IoT and cybersecurity segments in which HOMEPOT is positioned, and profiles the competitive landscape shaped by the five incumbent vendors (Microsoft, VMware, IBM, JAMF, and BlackBerry) alongside emerging regional players and open-source alternatives. The analysis identifies the four market drivers currently reshaping demand, examines the

	regulatory environment across the consortium's national footprint, and grounds each per-country market impact assessment in the corresponding demonstrator activity. The deliverable covers all seven consortium countries (Belgium, Czechia, Germany, Korea, Portugal, Türkiye, and the United Kingdom) and provides the analytical foundation on which D7.2 (Service Business Offerings) and D7.3 (Business Model Innovation and Validation) will build. The analysis reflects the CR3 baseline of November 2025.
Keywords:	Market analysis, Mobile Device Management, Unified Endpoint Management, Internet of Things, endpoint security, competitive landscape, market impact, NIS2, DORA, cybersecurity, business models, HOMEPOT

Revision No:	Content & Changes	Submission Date	Actual Submission Date
Version 1	First version of D7.1	May 2026	24 September 2026

Editors

Gofran Chowdhury

Contributors

Özer Aydemir
Tamer Berk
Tim Schürmann
Ayesha Nizam
Hale Gezgen
Ali Metin Balci
Maziar Ghorbani
Jongik Kim
Daesub Yoon
Janwillem Swalens
Ricardo Severino
Luis Gomes Andre
Luis Miguel Pinho
Jose Paulo Martins
Nicolas Gonzalez
Annanda Rath
Karel De Brabandere

Executive Summary

The HOMEPOT project addresses the growing complexity of managing heterogeneous IT and IoT devices, including edge and gateway systems. Devices from different manufacturers use different management interfaces, protocols, and operating systems, and organisations that operate mixed device fleets face fragmented tooling, inconsistent security postures, and rising operational cost. HOMEPOT is being developed as a Unified Endpoint Management (UEM) platform that bridges hardware, operating systems, and management interfaces, providing a single approach for managing devices that would otherwise require multiple separate tools.

The platform is designed to serve two audiences. For device manufacturers, HOMEPOT provides a route to producing devices that can be managed alongside those of other manufacturers in corporate environments. For operators, including corporate IT organisations, smart infrastructure developers, and MDM/UEM service providers, the platform enables the operation of heterogeneous device pools without dependence on a single vendor. HOMEPOT's distinctive positioning within the existing market is its extension of UEM principles to devices with dynamic and interactive user interfaces, including smartphones, computers, smart TVs, and kiosks, alongside the sensor-driven endpoints already covered by conventional IoT platforms.

D7.1 establishes the market baseline for Work Package 7 (Definition of New Business Models). It characterises the market in which HOMEPOT is positioned, profiles the competitive landscape, identifies the trends and gaps that shape demand, and grounds the analysis in the seven national demonstrator contexts. It does not propose commercial offerings, pricing structures, or business models. These are addressed in D7.2 (Service Business Offerings with the HOMEPOT Platform) and D7.3 (Business Model Innovation and Validation).

Global market conditions for HOMEPOT's target segment are favourable. The Mobile Device Management market, valued at approximately USD 11 billion in 2026, is projected to reach between USD 26 billion and USD 28 billion by 2030 and to exceed USD 30 billion by 2031. This implies a compound annual growth rate of 18.5% to 24.5% through the end of the decade (Mordor Intelligence, 2026; Grand View Research, 2025; The Insight Partners, 2025). Four drivers sustain this trajectory:

- The convergence of MDM, desktop management, and IoT management under Zero Trust architectures.
- The transition from predictive to autonomous, or agentic, AI in endpoint security.
- The surge in 5G-connected industrial and rugged IoT endpoints requiring specialised management profiles.
- The emergence of Digital Employee Experience (DEX) as a competitive differentiator in Bring-Your-Own-Device (BYOD) environments, now adopted by 82% of organisations.

The connected-device population underlying this market continues to expand. Omdia forecasts cellular IoT connections alone to reach 5.9 billion by 2035, while independent trackers already report more than 16 billion connected IoT devices worldwide. A significant proportion of these devices remains outside the effective reach of current UEM platforms, either because commercial management agents are too resource-intensive for constrained hardware or because existing platforms lack the vendor-independent policy abstractions required for heterogeneous fleets.

Competitive concentration in the MDM/UEM segment remains moderate. Five vendors, namely Microsoft, VMware (now under Broadcom), IBM, JAMF, and BlackBerry, collectively account for approximately 45% to 50% of global revenue. The remainder is contested by regional players, vertical specialists, and open-source alternatives. Recent market movement has been shaped by Broadcom's price increases following the VMware acquisition, which have triggered active customer re-evaluation, and by rising enterprise demand for cryptographic agility ahead of post-quantum standards adoption, sovereignty-flexible deployment under NIS2 and DORA, open APIs for integration with existing security stacks, and lightweight agents suitable for rugged and constrained devices. Incumbent platforms address these requirements unevenly, creating an opening for differentiated challengers.

HOMEPOT is positioned within this space. The project spans seven countries and includes nineteen partners covering the full value chain from academic research and OS development to cybersecurity provision, system integration, network operation, and end-user verticals. Each national demonstrator anchors the platform in a specific vertical and regulatory context:

- Belgium: renewable energy asset management (3E, SIRRIS, Nokia Bell N.V.).
- Czechia: heterogeneous industrial IT integration (EXPECT-IT).
- Germany: cross-border enterprise UEM (IOTIQ).
- Korea: mobility and location-based taxi dispatch (Essetel, ETRI, Chungnam National University).
- Portugal: telecom, IoT, and edge security (NOS Inovação, ISEP, Adyta).
- Türkiye: consumer electronics, banking-grade UEM, and critical infrastructure (ERSTE Software as project coordinator, Dakik Yazılım, KoçSistem, BLC, Arçelik).
- United Kingdom: hospitality and food service (GetFudo, Brunel University London, Dealdio).

Together, these demonstrators cover the majority of verticals driving current MDM market growth. The remainder of this deliverable presents the detailed market analysis, competitive assessment, and per-country impact evaluation supporting this positioning.

Table of Contents

2. Introduction

2.1. Purpose and Scope of D7.1

D7.1 is the first deliverable of Work Package 7 and represents the project's first formal analysis of the market in which HOMEPOT is positioned. Prior work packages have focused on the definition of requirements (WP2), the design of the reference architecture (WP3), the specification of data pipelines and analytical components (WP4), and the initial platform implementation (WP5). WP7 shifts the focus outward. Its role is to establish, in this deliverable, the market baseline that will support the definition of service offerings in D7.2 (Service Business Offerings with the HOMEPOT Platform, led by KoçSistem) and the validation of business models in D7.3 (Business Model Innovation and Validation, led by IOTIQ).

The deliverable serves five objectives:

- To characterise the market landscape relevant to HOMEPOT, covering UEM, MDM, IoT and edge device management, and adjacent cybersecurity segments.
- To identify the trends, opportunities, and challenges shaping demand in this market.
- To profile the competitive landscape and position HOMEPOT against incumbents and emerging alternatives.
- To assess market impact at the project, partner, and national levels.
- To provide the analytical baseline on which D7.2 and D7.3 will build.

The deliverable is descriptive and analytical in nature. It does not propose commercial offerings, pricing structures, or business models. These fall within the scope of the subsequent WP7 deliverables.

The analysis works from the current project baseline established under Change Request 3 (November 2025). Content from the original Full Project Proposal Annex has been retained where the underlying context remains valid, and has been revised or omitted where subsequent change requests have altered the consortium composition or refined the project scope.

2.2. Relationship to Other Work Packages

D7.1 draws on prior technical work rather than duplicating it. The relationships between D7.1 and the other work packages are summarised below.

- **WP2** (D2.1 Requirement Specification, D2.5 Identification of Support Technologies Classification): defines the functional scope of the platform and its supporting technology domains. Referenced in this deliverable where market claims require a technical anchor.
- **WP3** (D3.1 Architecture Requirements Definition, D3.2 HOMEPOT Reference Architecture Definition): defines the platform's architectural approach. Referenced when describing HOMEPOT's design differentiators against incumbent commercial solutions.
- **WP4** (D4.1 Data Specification and Acquisition) and **WP5**: define the analytical and implementation capabilities that translate into commercial value propositions.
- **WP6**: provides the demonstrator context on which the per-country market impact analysis in Section 8 is grounded.

- **WP8** (T8.2 Exploitation Plan, D8.1 Dissemination Plan, D8.3 Standardization Documentation): defines the exploitation, dissemination, and standardisation strategies that will carry HOMEPOT results into the market. T8.2 and D7.1 draw on shared partner-level material and must remain mutually consistent.

Within WP7, D7.1 provides the market baseline for D7.2 (Service Business Offerings) and D7.3 (Business Model Innovation and Validation). Together, the three deliverables constitute the WP7 output.

2.3. Methodology

- The market analysis is built from four sources of evidence.
- **Desk research on current market conditions.** Market sizing, competitive concentration, regional dynamics, and vertical breakdown draw on published analyst reports, including Mordor Intelligence (2026 base year), Grand View Research (2025), The Insight Partners (2025), Strategic Market Research (2024), ABI Research (2025), IndustryARC, Technavio, McKinsey, Omdia, and Transforma Insights. Regulatory analysis is based on the primary EU sources for the NIS2 Directive, DORA, GDPR, the Cyber Resilience Act, and the AI Act, together with the national frameworks relevant to specific demonstrators, including KVKK in Türkiye, PIPA in Korea, and the UK GDPR and NIS Regulations in the United Kingdom.
- **Consortium inputs.** Market analysis originally provided in the FPP Annex has been retained where still valid and revised in line with the CR3 baseline where necessary. WP7 discussion materials, including the 2026-2031 MDM market briefing prepared for recent WP7 meetings and the IoT market references circulated by consortium partners, have been incorporated where relevant.
- **Partner-level positioning aligned with the T8.2 Exploitation Plan.** Each partner's target market, competitive position, and intended exploitation pathway feed both D7.1 and T8.2. Where partner-specific content has not yet been consolidated at the time of this initial version, placeholders are used rather than assumed content.
- **Demonstrator-informed validation.** The seven national demonstrators (Belgium, Czechia, Germany, Korea, Portugal, Türkiye, and the United Kingdom) provide concrete deployment contexts against which market claims are validated. Each per-country market impact assessment in Section 8 is anchored in the corresponding demonstrator activity.

2.4. Document Structure

The remainder of this deliverable is organised as follows:

- **Section 3** presents the market landscape, including evolution from MDM to UEM, global market sizing, regional and vertical breakdown, component and deployment insights, key drivers, and the regulatory environment.
- **Section 4** analyses the competitive landscape, covering market concentration, dominant vendors, regional disruptors, gap areas, pricing dynamics, and HOMEPOT's competitive positioning.
- **Section 5** maps the HOMEPOT value chain and the consortium's position within it.

- **Section 6** identifies the target market segments across verticals, horizontals, and geographies.
- **Section 7** presents HOMEPOT's differentiators and the addressable market opportunity.
- **Section 8** provides the per-country market impact analyses.
- **Section 9** presents the consolidated market impact assessment.
- **Section 10** identifies risks, barriers, and mitigation measures.
- **Section 11** concludes and outlines the handover to D7.2 and D7.3.
- **Section 12** lists the references.
- **Annex A** provides the consortium partner list. **Annex B** lists acronyms and abbreviations used throughout the document.

3. Market Landscape

3.1. Evolution from MDM to EMM to UEM

The management of enterprise devices has evolved through three overlapping phases. Mobile Device Management (MDM) emerged in response to the growing use of smartphones and tablets in corporate environments and focused on the enforcement of security policies, remote configuration, and the ability to wipe lost or compromised devices. As device pools diversified, MDM proved insufficient on its own, and Enterprise Mobility Management (EMM) extended the discipline to include Mobile Application Management (MAM) and Mobile Content Management (MCM). Unified Endpoint Management (UEM) represents the current consolidation, bringing smartphones, tablets, laptops, desktops, wearables, IoT devices, and edge or gateway systems under a single management platform, independent of operating system or manufacturer.

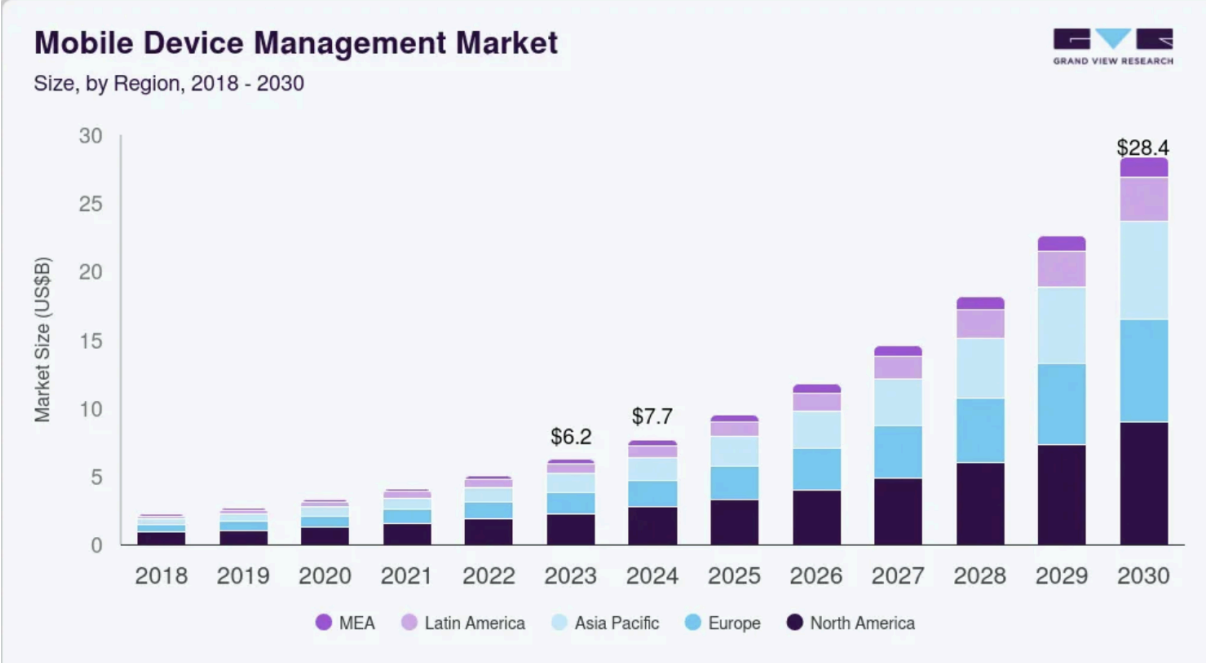
The core capabilities of UEM platforms span device lifecycle management, application management, security and compliance enforcement, identity and access management (IAM), data containerisation, remote support, and analytics. Current-generation platforms are extending beyond this baseline into what recent analysis describes as "Intelligent Endpoint Resilience" (Strategic Market Research, 2024), combining UEM capabilities with agentic artificial intelligence, behavioural analytics, and cryptographic foundations positioned for the post-quantum transition.

3.2. Global Market Sizing and Growth

The global Mobile Device Management market entered a phase of rapid acceleration in the mid-2020s. Mordor Intelligence estimates the global MDM market at approximately USD 11 billion for the 2026 base year, having grown from USD 6.2 billion in 2023 and USD 7.7 billion in 2024, as reported by Grand View Research. Forecast trajectories from three independent sources converge on continued strong growth through the end of the decade and into 2031.

Year	Market size (USD)	Source
2023	6.2 B	Grand View Research
2024	7.7 B	Grand View Research
2026	~11 B (base year)	Mordor Intelligence
2030	26.04 B	Mordor Intelligence
2030	28.37 B	Grand View Research
2031	> 30 B	The Insight Partners

The implied compound annual growth rate across these projections ranges from 18.5% to 24.5% through 2031, depending on the source. While the CAGR has moderated from the 26.1% figure reported at the time of the FPP submission (MarketsandMarkets, 2023), the absolute expansion of the market remains substantial, with the market more than doubling between 2026 and 2030.



Mobile Device Management Market Size by Region, 2018-2030, Grand View Research

Adjacent market segments relevant to HOMEPOT extend the addressable landscape beyond the MDM core. IoT device management platforms are projected to grow at double-digit CAGRs, driven by industrial IoT, smart city, and energy applications. Cybersecurity for distributed and heterogeneous systems is expanding under the pressure of NIS2, DORA, supply-chain risk frameworks, and the convergence of IT and OT environments. Edge computing and Multi-Access Edge Computing (MEC) continue to expand, supporting the deployment of management capabilities close to constrained

devices. Vertical digital platforms in energy, mobility, smart buildings, retail, and hospitality are increasingly interdependent with endpoint management.

The underlying connected-device population continues to expand rapidly. Omdia forecasts cellular IoT connections alone to reach 5.9 billion by 2035, while IoT Analytics reports more than 16 billion connected IoT devices globally in the mid-2020s. Transforma Insights and Research Nester project sustained growth in the IoT solutions and services market throughout the forecast horizon. The scale of the connected-device population defines the ultimate ceiling of the endpoint management opportunity, a significant portion of which remains outside the effective reach of current UEM platforms.

3.3. Regional Dynamics

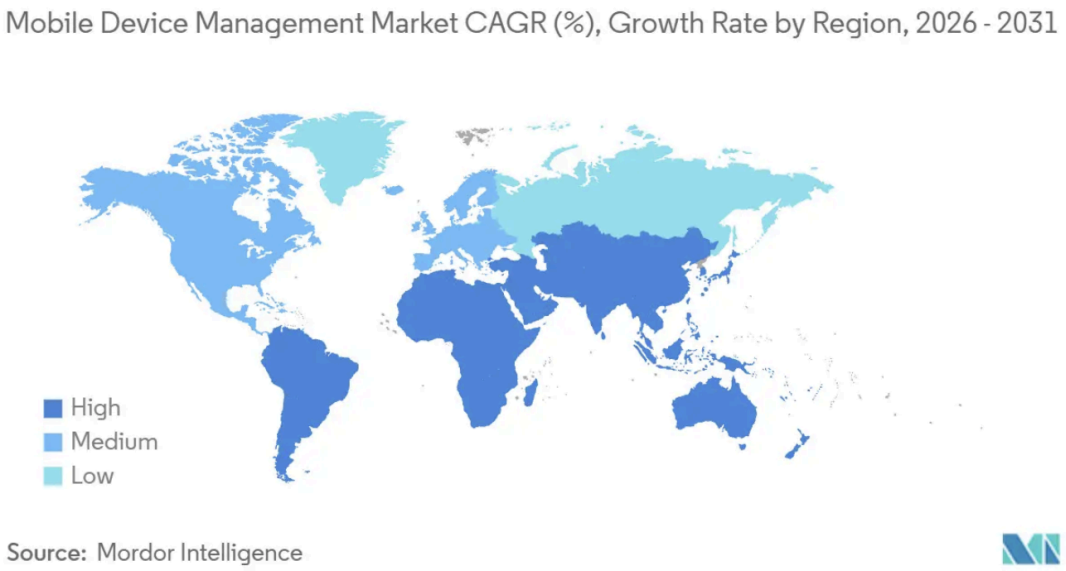
Regional market dynamics vary significantly in both scale and rate of growth.

North America retains the largest share of the MDM market, at approximately 39% of global revenue (Mordor Intelligence, 2026). The region's dominance is sustained by early 5G adoption, mature enterprise IT infrastructure, the concentration of major vendors including Microsoft, IBM, and VMware, and demand driven by strict compliance frameworks such as HIPAA and SOX. High levels of hybrid-work maturity have consolidated UEM as a standard component of enterprise IT operations.

Asia-Pacific is the fastest-growing region, with a CAGR of approximately 28.1% through 2031. The region is the primary engine of global market expansion during this period. Digitalisation in India and China accounts for a substantial share of this growth. Research & Markets (2024) forecasts the Chinese MDM market alone to reach USD 5 billion by 2030, at an individual CAGR of 34.3%. This dynamic is directly relevant to the international expansion pathways of the Korean sub-consortium.

Europe shows steady expansion, driven principally by data sovereignty requirements. The GDPR, NIS2, and DORA regulatory frameworks impose obligations relating to localised data hosting, encryption, and operational resilience, favouring platforms capable of demonstrating jurisdictional control. This regulatory environment represents a structural tailwind for European-developed platforms, including HOMEPOT.

The Middle East and Africa and Latin America represent smaller but growing markets. Türkiye's geographic position places its consortium partners in a bridging role between European regulatory norms and the Middle Eastern, Central Asian, and North African markets.



Mobile Device Management Market CAGR Growth Rate by Region, 2026-2031, Mordor Intelligence

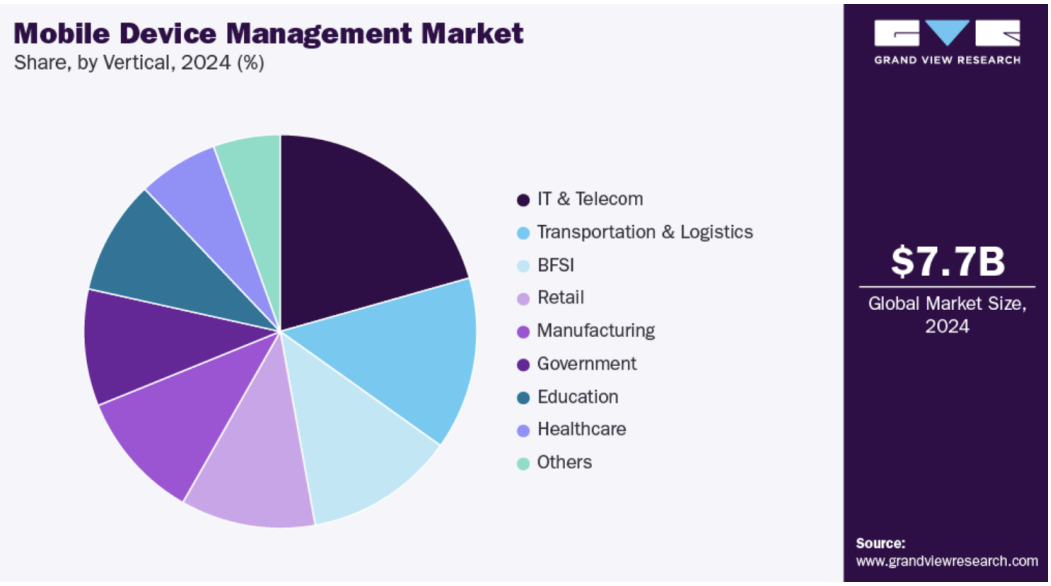
3.4. Vertical Breakdown

MDM adoption varies substantially across industry verticals, with sector-specific compliance requirements and operational drivers shaping demand.

Vertical	Share or growth indicator	Principal drivers
Healthcare	~24.5% share (largest vertical)	Telemedicine tablets, wearable patient monitors, HIPAA compliance (IndustryARC, 2024)
BFSI	High value	Mobile banking application security, fraud prevention via compromised endpoints (Grand View Research, 2025)
Manufacturing	54.1% CAGR (5G endpoints)	Industrial robots, smart factory sensors, ruggedised handhelds (ABI Research, 2025)
Retail	Rising adoption	Mobile Point-of-Sale, digital signage, warehouse automation (Strategic Market Research, 2024)
Education	Increasing share	1:1 student device programmes, remote learning platforms (Technavio, 2025)
IT and Telecom	Largest single share of 2024 vertical mix	Internal IT estate management

Transportation and Logistics	Major share	Fleet device management
Government	Significant share	Public-sector device pools

The 2024 vertical mix reported by Grand View Research shows IT and Telecom, Transportation and Logistics, BFSI, and Manufacturing as the largest revenue contributors. This distribution maps closely onto the vertical coverage of the HOMEPOT demonstrators, which span hospitality and food service (United Kingdom), consumer electronics and critical infrastructure (Türkiye), renewable energy (Belgium), mobility (Korea), telecom and IoT (Portugal), industrial IT integration (Czechia), and cross-vertical enterprise UEM (Germany). Vertical alignment is examined in greater depth in Section 6.



Mobile Device Management Market Share by Vertical, 2024, Grand View Research

3.5. Component and Deployment Insights

Two structural characteristics of the market are relevant to HOMEPOT's positioning.

- Cloud-based deployment now accounts for approximately 62.4% of the global market (Strategic Market Research, 2024). The Software-as-a-Service model has become the default enterprise approach, valued for its ability to distribute security updates in real time across geographically dispersed workforces. On-premises deployment retains a role in regulated sectors and in environments with strict data residency requirements.
- The market divides between software and services, with software accounting for over 63% of current revenue. The services segment, comprising managed services and consulting, is growing more rapidly, at a CAGR of 27.3% (Grand View Research, 2025). This differential is driven principally by a global shortage of in-house cybersecurity expertise, which pushes organisations toward outsourced management arrangements. The rapid growth of the

services segment represents a structural opportunity for managed-service offerings built around the HOMEPOT platform, addressed in D7.2.

3.6. Key Market Drivers

Four convergent drivers define the current phase of MDM/UEM market development. The following synthesis draws on Strategic Market Research (2024), McKinsey (2025), ABI Research (2025), and The Insight Partners (2025).

1. **Convergence under Zero Trust.** MDM is no longer treated as a standalone discipline. It is being integrated with desktop and IoT management into single-pane-of-glass UEM platforms, in support of Zero Trust architectures that require continuous device verification. This convergence raises the technical bar for management platforms and rewards those able to cover heterogeneous device pools consistently.
2. **Agentic AI in security.** Artificial intelligence in endpoint security is transitioning from predictive alerting to autonomous action. Modern platforms increasingly neutralise threats such as data exfiltration and unauthorised SIM swaps in real time, without direct IT intervention. The shift affects both product architecture and operating model expectations.
3. **5G and IoT synergy.** The rollout of 5G standalone networks is driving a surge in connected rugged and industrial devices. These endpoints require specialised management profiles suited to low-latency, high-reliability industrial use cases in manufacturing, logistics, and infrastructure. The pattern is directly relevant to Belgian energy, Korean mobility, and UK distributed-site demonstrators.
4. **Digital Employee Experience.** BYOD arrangements are now reported by 82% of organisations. In response, vendors are increasingly competing on the invisibility of management overlays, combined with strict containerisation of corporate data, in order to address employee privacy concerns. This driver is relevant to HOMEPOT's user-interface and adaptive management objectives.

3.7. Regulatory and Compliance Drivers

Regulation is a structural driver of UEM adoption in Europe and, increasingly, in the national markets in which HOMEPOT partners operate. The principal frameworks are summarised below.

- **NIS2 Directive** (Directive (EU) 2022/2555). Broadens the scope of entities designated as essential or important and imposes cybersecurity obligations that directly affect energy, transport, healthcare, and digital infrastructure operators. NIS2 is a major driver of European UEM adoption.
- **Digital Operational Resilience Act** (Regulation (EU) 2022/2554). Extends operational resilience requirements to the financial services sector, creating specific demand for auditable endpoint management in banking and insurance.
- **General Data Protection Regulation** (Regulation (EU) 2016/679). Continues to shape the handling of personal data on managed devices.
- **Cyber Resilience Act** (Regulation (EU) 2024/2847). Imposes security obligations on products with digital elements, including devices managed by UEM platforms.
- **Artificial Intelligence Act** (Regulation (EU) 2024/1689). Relevant to the AI components integrated in HOMEPOT for adaptive management and anomaly detection.

- **National frameworks.** These include KVKK (Türkiye), PIPA (Korea), UK GDPR and the UK NIS Regulations (United Kingdom), and sector-specific frameworks equivalent to HIPAA in healthcare.

The cumulative effect of this regulatory environment is to favour platforms capable of demonstrating jurisdictional data control, auditability, and cryptographic agility. Each of these characteristics aligns with HOMEPOT's architectural approach, and their commercial implications are examined in Sections 4 and 7.

4. Competitive Landscape

4.1. Market Concentration

The MDM/UEM market is currently characterised as moderately concentrated (Mordor Intelligence, 2026). A small group of established vendors accounts for the largest share of global revenue, while a broader second tier of specialised, regional, and open-source providers competes on price, vertical depth, and localised support. The structure is neither a stable oligopoly nor a fully fragmented field. It is a configuration that rewards differentiated challengers capable of addressing specific gap areas rather than attempting to displace incumbents in their established segments.

The five leading vendors, Microsoft, VMware (operating under Broadcom), IBM, JAMF, and BlackBerry, collectively capture between 45% and 50% of global revenue. The remaining share is contested by a diverse group of vendors with distinct competitive strategies, examined in the sections that follow.

4.2. The Five Dominant Vendors

The competitive positioning of the five dominant vendors is summarised below, together with the principal strengths and vulnerabilities identified in the current market analysis (Mordor Intelligence, 2026; McKinsey, 2025).

Vendor	Positioning	Strengths	Vulnerabilities
Microsoft (Intune)	Cross-sold via Microsoft 365 and Entra (Azure AD)	Entrenched identity base; Windows Autopilot zero-touch provisioning	Limited coverage for non-Microsoft device classes; weak IoT depth
VMware Workspace ONE (Broadcom)	Integration of virtualisation, device management, and security analytics	Mature cross-platform UEM; deep enterprise footprint	15% to 20% price increase post-acquisition triggering active customer churn
IBM MaaS360	AI-augmented UEM with Watson AI	Global telemetry; mature anomaly detection	Mid-to-large enterprise focus; limited SMB traction

JAMF	Apple-only ecosystem specialist	Hardware-backed attestation; strong presence in creative and education sectors	Single-vendor scope by design
BlackBerry	Security-first heritage	Established position in regulated and government sectors	Declining market share over the past decade

Microsoft's dominant position in the Windows-centric enterprise segment is reinforced by its ability to cross-sell Intune through Microsoft 365 subscriptions. This bundling advantage is significant in organisations already committed to the Microsoft ecosystem but does not extend readily to environments with substantial IoT, non-Microsoft, or vendor-diverse device populations.

VMware Workspace ONE, following its acquisition by Broadcom, has retained a mature cross-platform capability but is currently the source of the market's most visible pricing disruption. Price increases of 15% to 20% following the integration of Workspace ONE with Symantec have triggered widespread customer re-evaluation, creating a substantial pool of enterprises actively considering alternative platforms. The commercial implications of this dynamic are examined in Section 4.5.

IBM MaaS360 differentiates on the integration of Watson AI for anomaly detection and threat identification, drawing on IBM's global telemetry. Its market position is concentrated in mid-to-large enterprises rather than the small and medium-sized enterprise (SME) segment.

JAMF maintains a specialist position focused exclusively on the Apple ecosystem, sustained by hardware-backed attestation and strong customer bases in creative and educational sectors. Its narrow scope is both a defensive advantage within its target segment and a limitation on total addressable market.

BlackBerry retains presence in regulated and governmental sectors, supported by its security heritage, but its share of the broader UEM market has declined progressively over the past decade.

4.3. Emerging Regional Disruptors

A second tier of vendors is capturing meaningful share in the SME segment across India and Southeast Asia. These providers compete on the basis of lightweight, easily deployed management agents and customer support delivered in local languages, addressing markets in which the five dominant vendors are typically less effective. The pattern is directly relevant to two elements of HOMEPOT's international positioning. First, the Korean sub-consortium has identified Southeast Asia as its principal expansion target, aligning with the strongest regional growth in Asia-Pacific. Second, the Turkish sub-consortium's geographic position enables it to serve as a bridge between European regulatory norms and the Central Asian and Middle Eastern markets, where similar lightweight-agent, localised-support dynamics apply.

4.4. Gap Areas and Innovation Frontiers

Two acute gap areas in the current vendor landscape are of particular relevance to HOMEPOT's positioning (Mordor Intelligence, 2026).

- **The rugged IoT gap.** Standard MDM agents remain too resource-intensive for rugged IoT endpoints, resulting in significant battery drain and operational overhead. This represents an underserved market segment in which specialised, low-power management approaches are required. HOMEPOT's abstract policy mediator design and its edge-cloud collaboration model are directly aligned with this requirement.
- **The cryptographic race.** Following the standardisation of post-quantum cryptography by NIST (FIPS 203, 204, and 205), vendors with substantive in-house cryptographic expertise are expected to gain long-term competitive advantage. Cryptographic agility, defined as the ability to transition between cryptographic primitives without architectural rework, is emerging as a differentiator in enterprise procurement. HOMEPOT's consortium includes cybersecurity specialists (BLC, Adyta, SIRRIS) whose expertise supports this positioning.

4.5. Pricing Dynamics and Churn Risk

The current MDM/UEM market exhibits a "churn dynamic" rather than a stable oligopolistic pattern (Mordor Intelligence, 2026). Two developments are relevant.

The first is the pricing disruption associated with Broadcom's post-acquisition strategy for VMware Workspace ONE. The 15% to 20% price increase applied following the integration of Workspace ONE with Symantec has triggered widespread customer re-evaluation, particularly among large enterprises with existing VMware commitments. This has created a substantial pool of enterprises actively considering alternative platforms.

The second is the emergence of carrier-integrated UEM offerings. Telecommunications operators, including Verizon and AT&T, are increasingly bundling MDM capabilities into 5G data plans, providing security enforcement at the network-slice level. This development is directly relevant to the Portuguese sub-consortium, in which NOS Inovação combines telecom operator status with a system-integration role, and to the Korean sub-consortium's mobility-focused positioning.

The strategic implication supported by current analyst commentary is that innovation in this market has moved beyond feature parity. Services-led differentiation, anchored in cryptographic agility, API openness, and sovereignty flexibility, is now the principal determinant of customer retention. Each of these dimensions aligns with HOMEPOT's design principles.

4.6. Competitive Positioning of HOMEPOT

HOMEPOT does not seek to displace incumbent UEM vendors in their established enterprise segments. Its differentiated positioning targets specific gap areas that commercial platforms address only partially. The following seven positioning elements together define HOMEPOT's competitive stance.

1. **Heterogeneous device pools.** HOMEPOT is designed to manage traditional IT endpoints, IoT devices, edge and gateway systems, and devices with interactive user interfaces (smartphones, computers, smart TVs, kiosks, in-vehicle screens) under a single management plane.
2. **Vendor-independent device pools.** The abstract policy mediator decouples management semantics from device-specific APIs, breaking manufacturer lock-in and creating portability advantages in a market currently affected by the Broadcom pricing disruption.
3. **Vertical-specific deployments.** HOMEPOT's demonstrator coverage across energy, mobility, hospitality, food service, education, and healthcare provides validated vertical extension paths that horizontal UEM platforms typically require heavy customisation to achieve.
4. **EU regulatory compliance by design.** The platform is architected to support NIS2 and DORA compliance, with sovereignty-flexible deployment options.
5. **Edge-cloud collaboration.** HOMEPOT's design supports management capabilities in latency-sensitive and intermittently connected deployments, extending effective reach beyond centrally hosted models.
6. **Cryptographic and post-quantum readiness.** The policy mediator architecture and the involvement of dedicated cybersecurity partners support cryptographic agility ahead of enterprise-scale post-quantum transition.
7. **Rugged IoT efficiency.** The abstract, lightweight policy enforcement model is suited to resource-constrained endpoints, addressing the rugged IoT gap identified in Section 4.4.

The mapping between these positioning elements and HOMEPOT's technical solutions is examined in Section 7. The consortium's ability to deliver on this positioning across the value chain is examined in Section 5.

5. HOMEPOT Value Chain and Ecosystem

5.1. Value Chain Overview

The commercial deployment of a UEM platform such as HOMEPOT depends on the coordinated participation of multiple actors across a well-defined value chain. The value chain identified for HOMEPOT, drawing on the original analysis in the FPP Annex and refined in the CR3 baseline, comprises eleven roles.

- **Research and academic institutions** contribute fundamental research, algorithms, and independent validation.
- **Device manufacturers** originate the hardware managed by the platform and define the interfaces through which management occurs.
- **Operating system providers and developers** supply the OS substrate on which devices operate and against which management policies are enforced.
- **UEM service providers** deliver management capability to end users, either as software licences or as managed services.
- **Cybersecurity service providers** supply security overlays, incident response, and specialised protection layers.
- **Infrastructure-as-a-Service and Platform-as-a-Service providers** supply the cloud substrate on which centralised management components run.

- **SaaS solution providers** package platform capabilities as subscription-based managed offerings.
- **System integrators** deploy, customise, and integrate the platform into end-user environments.
- **Network operators** provide the connectivity that binds the managed device population to the management infrastructure, including 5G and edge connectivity.
- **Value-Added Service (VAS) providers** deliver domain-specific services built on top of the platform.
- **End users** operate the managed device populations across enterprise, public sector, healthcare, education, and hospitality environments.

HOMEPOT Market Value Chain

The commercial significance of the value chain, from D7.1's perspective, is that any UEM platform lacking coverage of one or more of these roles will depend on external partners to reach the market. HOMEPOT's consortium composition provides internal coverage of every role identified above. The mapping between roles and consortium partners is presented in Section 5.2.

5.2. Role Mapping Across Consortium Partners

The consortium comprises nineteen partners distributed across seven countries. The distribution of partners across the value chain roles is summarised below.

Value chain role	Partners
Research and academia	SIRRIS (BE), Brunel University London (UK), ISEP (PT), Chungnam National University (KR), ETRI (KR)

UEM and OS provision	ERSTE Software (TR), Dakik Yazılım (TR), IOTIQ (DE)
Cybersecurity provision	BLC İletişim ve Güvenlik (TR), Adyta (PT)
Device manufacturers	Arçelik (TR)
Cloud and SaaS infrastructure provision	EXPECT-IT (CZ), BLC (TR), Nokia Bell N.V. (BE)
System integration and managed services	KoçSistem (TR), EXPECT-IT (CZ), NOS Inovação (PT)
Network operators	NOS Inovação (PT)
VAS and application providers	3E (BE, renewable energy), GetFudo (UK, food service), Dealdio (UK, loyalty and application technology), Essetel (KR, mobility), Arçelik (TR, consumer electronics and smart room)
End-user verticals	All demonstrator partners

The consortium covers every value chain role internally, from academic research through operating system development, cybersecurity, cloud and SaaS provision, system integration, network operation, value-added service delivery, and end-user application. This internal coverage is significant commercially because it enables partner-led exploitation across multiple layers of the market without dependence on external contractors, and because it supports the delivery of composite offerings in which multiple partners contribute in coordinated fashion.

5.3. Inter-Partner Synergies

The consortium composition supports a range of joint exploitation opportunities that individual partners would find difficult to pursue alone. The synergies identified in the FPP Annex, restricted here to the current CR3 partner set, are summarised below.

- **3E with BLC, Dakik Yazılım, Arçelik, SIRRIS, and Nokia Bell N.V.** Standardised remote control of energy and HVAC assets, secure bi-directional communication for renewable energy sites, and shared work on industrial endpoint monitoring.
- **Adyta with ISEP and NOS Inovação.** Joint development of IoT security solutions within the Portuguese ecosystem, combining research, network operator infrastructure, and specialised cybersecurity provision.
- **Arçelik with ERSTE Software.** The Smart Room Experience concept, integrating manageable smart devices for hospitality, healthcare, and education environments.
- **BLC with 3E and Dakik Yazılım.** An open-source cloud environment based on OpenStack and Kubernetes, positioned to serve as an edge processing platform for 5G vertical applications including Vehicle-to-Everything communications, port automation, and smart city deployments.

- **Dakik Yazılım with ERSTE Software and BLC.** An integrated UEM offering with advanced security features, forming the technical core of the Turkish sub-consortium's joint exploitation pathway.
- **Dealdio with Arçelik, ERSTE Software, Dakik Yazılım, and KoçSistem.** Integration of loyalty and rewards capabilities into smart TV applications and MDM offerings, establishing a commercial bridge between the UK and Turkish sub-consortia.
- **ERSTE Software with Dakik Yazılım and Arçelik.** An integrated UEM offering covering consumer goods, enterprise IT, and customised operating systems.
- **Essetel with ETRI and Chungnam National University.** The Korean taxi-calling cross-platform service, combining commercial deployment, research-to-commercialisation transfer, and academic research.
- **IOTIQ with ERSTE Software and Dakik Yazılım.** Cross-border UEM exploitation between Germany and Türkiye, grounded in the German WP7 leadership responsibility for business model definition.
- **GetFudo with Dealdio and Brunel University London.** The UK food service deployment, combining commercial use case delivery, application and loyalty technology, and academic validation through modelling, simulation, and VVUQ techniques.
- **EXPECT-IT with all WP6 partners.** Czech-led integration and evaluation of the platform across all national demonstrators, providing the central role of coordinating the demonstrator programme end-to-end.

Each of these synergies represents both a technical collaboration path and a commercial exploitation opportunity. The relationship between partner-level exploitation and the consolidated project-level market impact is examined in Sections 8 and 9. Detailed partner-level exploitation plans, including planned commercial pathways and target customer segments, are maintained within the T8.2 Exploitation Plan and are not duplicated here.

6. Target Market Segments

6.1. Vertical Segments

HOMEPOT's addressable market is defined by the intersection of two factors: the verticals in which endpoint management demand is growing most strongly, and the verticals in which the consortium has direct demonstrator coverage. The verticals identified below are drawn from the current market analysis presented in Section 3.4, mapped to HOMEPOT's demonstrator programme.

Energy. The Belgian demonstrator, delivered by 3E in collaboration with SIRRIS and Nokia Bell N.V., targets renewable energy asset management, smart metering, and the secure remote control of grid edge devices. The vertical is directly affected by the EU NIS2 essential-entity requirements and by the European renewable energy capacity targets for 2030. Both factors sustain demand for secure endpoint management capabilities in this segment.

Mobility and transport. The Korean demonstrator, delivered by Essetel with ETRI and Chungnam National University, targets location-based services and taxi dispatch, with fleet management as an adjacent extension. The vertical intersects with the manufacturing and IoT segments that show the highest CAGR in the current market, driven by 5G-connected industrial and logistics endpoints.

Hospitality and food service. The UK demonstrator, delivered by GetFudo with Dealdio and Brunel University London, targets Point-of-Sale terminals, kiosks, kitchen systems, and delivery tablets across multi-site restaurant operations. The vertical is aligned with the rising retail adoption trend identified in the market data and represents a segment in which incumbent UEM platforms typically require heavy customisation to serve.

Consumer electronics and smart environments. Arçelik's participation as a device manufacturer, together with ERSTE Software and Dakik Yazılım, addresses the management of smart TVs, kiosks, and other consumer-electronics devices deployed in corporate hospitality, healthcare, and education environments. This vertical is central to HOMEPOT's differentiated positioning around devices with dynamic user interfaces.

Consumer goods and light industry. ERSTE Software's engagement with ETİ in Türkiye covers UEM for confectionery production lines and distribution. The vertical intersects with the broader manufacturing segment, where 5G endpoint growth is strongest.

Telecom and IoT. The Portuguese demonstrator, delivered by NOS Inovação with ISEP and Adyta, targets IoT and edge security in operator-managed environments. The vertical is directly connected to the emerging carrier-integrated UEM trend identified in Section 4.5, in which telecommunications operators bundle management capabilities into 5G data plans.

Industrial IT integration. The Czech demonstrator, delivered by EXPECT-IT, addresses the operational management challenges arising from complex IT systems built from components supplied by multiple manufacturers. The vertical corresponds to the enterprise IT and Telecom segment identified in the market vertical mix as the single largest revenue contributor in 2024.

Financial services (BFSI). ERSTE Software's engagement with Ziraat Katılım in Türkiye demonstrates banking-grade UEM under stringent financial-sector compliance requirements. The vertical is a direct beneficiary of DORA-driven demand for auditable endpoint management, and is characterised as high-value in the current market analysis.

Public sector and critical infrastructure. Turkish partners including BLC and KoçSistem address critical infrastructure sectors including energy, transportation, telecommunications, and public services. The vertical is aligned with NIS2 obligations and with the substantial share attributed to the government segment in the 2024 vertical mix.

Healthcare and education. Both verticals appear in the market data as significant and growing segments (healthcare at approximately 24.5% share, education increasing share). HOMEPOT's coverage in these verticals arises indirectly through the Smart Room Experience concept (Arçelik and ERSTE Software) and through Turkish engagements addressing regulated environments. Diakonie in Germany, addressed through ERSTE Software, provides a specific point of engagement in social services data protection.

6.2. Horizontal Segments

Across the verticals identified above, three horizontal customer segments are relevant to HOMEPOT.

- **Enterprises and small and medium-sized enterprises.** Organisations operating heterogeneous IT and IoT device populations represent the primary target for HOMEPOT's core platform. The segment is characterised by mixed operating systems, multiple vendor relationships, and rising compliance obligations. Enterprises currently affected by the Broadcom pricing disruption examined in Section 4.5 constitute an accessible sub-segment of active buyers.
- **Public sector and municipalities.** Public-sector organisations, including municipalities, require compliant management of large-scale device populations across administrative, educational, and public-service contexts. The segment is sensitive to sovereignty, procurement transparency, and vendor-independence considerations, each of which aligns with HOMEPOT's design principles.
- **Managed service providers.** MSPs delivering UEM-as-a-service constitute an indirect but strategically significant segment. The 27.3% CAGR reported for the services segment of the MDM market (Section 3.5) is driven substantially by MSP-delivered offerings. HOMEPOT's positioning as a platform for MSP-delivered services rather than exclusively as a direct-sale product supports engagement with this segment.

6.3. Geographic Priority Markets

The consortium's national footprint defines HOMEPOT's primary geographic priority markets. Belgium, Czechia, Germany, Korea, Portugal, Türkiye, and the United Kingdom each represent a national context in which at least one consortium partner is directly active. Beyond these primary markets, three cross-cutting geographic observations are relevant to the wider addressable opportunity.

- **European market coverage** is reinforced by regulatory demand. NIS2, DORA, and GDPR create structural demand for sovereignty-flexible platforms across the entire European market, extending HOMEPOT's addressable geography significantly beyond the four European consortium countries.
- **Asia-Pacific expansion**, focused on Southeast Asia, has been identified by the Korean sub-consortium as its principal international priority. The region is aligned with the 28.1% CAGR forecast for Asia-Pacific through 2031 and represents the highest-growth geography identified in the current market analysis.
- **Central Asia, the Middle East, and North Africa** are accessible through the Turkish sub-consortium's geographic position. The pattern identified in Section 4.3, in which regional disruptors capture SME share through lightweight agents and localised support, applies directly to this expansion pathway.

The consolidated market impact across geographies and verticals is examined in Section 9. Country-specific market impact assessments, including partner-level exploitation contexts, are presented in Section 8.

7. HOMEPOT Differentiators and Market Opportunity

7.1. Problem Solution Mapping

The HOMEPOT project is structured around a set of core problems identified during the requirements definition phase and translated into seven technical solutions incorporated into the platform architecture. The mapping between problems and solutions is summarised below and forms the technical basis for the differentiation analysis presented in this section.

Problem	HOMEPOT solution(s)	Corresponding market gap
P1 — Device diversity	S1, S4, S7	Incumbent UEM platforms address heterogeneous device pools unevenly, particularly where IoT, edge, and interactive-UI devices coexist with conventional IT endpoints.
P2 — Manufacturer preferences	S1, S6	Vendor lock-in is reinforced by device-specific management APIs, creating switching costs that affect both manufacturers and operators.
P3 — Specialised use cases	S3, S4, S7	Horizontal UEM platforms require substantial customisation to serve vertical-specific deployments in energy, mobility, hospitality, and healthcare.
P4 — Rapid evolution and competition	S1, S4	The rate at which device APIs change exceeds the release cadence of major UEM platforms, creating recurrent integration debt.
P5 — Market and cost constraints	S1, S7	Per-device licensing models scale poorly for organisations operating large IoT and edge device populations.
P6 — Security and compatibility	S2a, S2b, S5	Heterogeneity in device pools introduces inconsistencies in security posture, complicating compliance under NIS2 and DORA.

The seven HOMEPOT solutions referenced above are: S1 Policy Mediator, S2a Advanced IoT monitoring and detection, S2b Location-based authentication layer, S3 Machine-learning-based adaptive MDM features, S4 Cross-OS consistency, S5 Responsible AI and trustless data monetisation, S6 Device ecosystem compatibility, and S7 Device-independent abstract policy.

The essential characteristic of the problem-solution mapping is that each of the six problems corresponds to a market gap identified in the competitive analysis in Section 4. HOMEPOT does not attempt to displace incumbent platforms in their established areas of strength. Rather, it addresses the specific gap areas where those platforms are structurally limited. This alignment between

technical solutions and market gaps is what supports the addressable market estimate presented in Section 7.3.

7.2. Unique Value Propositions

- HOMEPOT's unique value propositions arise from the intersection of its technical solutions and the current state of the market. Seven value propositions are identified.
- **Policy abstraction across heterogeneous device pools.** HOMEPOT provides a single management plan for IT, IoT, edge, gateway, and interactive-UI devices. This value proposition addresses the fundamental problem articulated in the project's original concept, in which the proliferation of manufacturer-specific management interfaces is likened to the use of a separate remote control for each device. The policy abstraction approach is directly aligned with the rugged IoT gap identified in Section 4.4.
- **Vendor independence and portability.** The abstract policy mediator decouples management semantics from device-specific APIs. This creates portability advantages for operators seeking alternatives in the current market, particularly among enterprises affected by the Broadcom pricing disruption examined in Section 4.5.
- **Dual-audience positioning.** HOMEPOT is designed to serve device manufacturers seeking to produce devices that can be managed alongside those of other manufacturers, and operators seeking to run heterogeneous device pools without single-vendor dependence. The dual-audience positioning is a distinctive feature of the platform and is reflected in the consortium composition through the presence of both device manufacturers and system integrators.
- **European regulatory alignment by design.** The platform is architected to support NIS2, DORA, and GDPR compliance, with sovereignty-flexible deployment. This alignment corresponds directly to the structural regulatory tailwind identified for the European market in Section 3.3.
- **Cryptographic agility readiness.** The policy mediator architecture and the involvement of dedicated cybersecurity partners support the anticipated enterprise transition to post-quantum cryptographic standards. This positioning is aligned with the cryptographic race identified as an emerging differentiator in Section 4.4.
- **AI-driven adaptive management and anomaly detection.** HOMEPOT integrates AI capabilities for adaptive user interfaces, anomaly detection, and predictive management. The approach is aligned with the shift from predictive to agentic AI examined in Section 3.6.
- **Edge-cloud collaboration with lightweight footprint.** The platform's design supports management capabilities in latency-sensitive and intermittently connected deployments, and its abstract policy enforcement is suited to resource-constrained endpoints. Both characteristics address the rugged IoT gap.

The seven value propositions are distinct but reinforcing. Together they define a competitive space that is not fully occupied by any current commercial platform.

7.3. Addressable Market Estimate

- The addressable market for HOMEPOT is defined in three concentric layers, following the standard Total Addressable Market (TAM), Serviceable Available Market (SAM), and Serviceable Obtainable Market (SOM) framework.
- **Total Addressable Market.** HOMEPOT's TAM comprises the global MDM/UEM market together with adjacent segments in IoT device management and endpoint-focused managed cybersecurity services. On the baseline established in Section 3.2, the global MDM market alone is projected to reach between USD 26 billion and USD 28 billion by 2030, and to exceed USD 30 billion by 2031. Adjacent IoT device management platforms are projected to grow at double-digit CAGRs, and the managed cybersecurity services segment grows at 27.3% CAGR (Section 3.5). The indicative TAM for HOMEPOT's relevant slice of these combined segments is in the range of USD 35 billion to USD 45 billion by 2030.
- **Serviceable Available Market.** HOMEPOT's SAM comprises the portion of the TAM that is directly addressable through the consortium's geographic footprint and vertical positioning. This includes the European market, in which regulatory demand under NIS2 and DORA provides structural support, and the specific national markets of Türkiye, Korea, and the United Kingdom, in which consortium partners maintain direct commercial presence and identified expansion pathways. Vertical scope is defined by the coverage established in Section 6.1. Quantification of SAM at the partner level requires input from the T8.2 Exploitation Plan and is deferred to the consolidated exercise conducted jointly with WP7 partners.
- **Serviceable Obtainable Market.** HOMEPOT's SOM represents the realistic share of SAM that can be captured during the three-to-five-year period following project completion. Estimation of SOM depends on the specific service offerings defined in D7.2 and the business models validated in D7.3, and is therefore not finalised in this deliverable. Preliminary partner-level estimates aligned with the T8.2 Exploitation Plan will inform the SOM figure in subsequent WP7 outputs.

The three-layer estimate above establishes the market opportunity envelope within which HOMEPOT is positioned. It is not intended as a commercial projection. The purpose of the estimate at this stage of Work Package 7 is to demonstrate that the addressable opportunity is sufficient to support the exploitation pathways identified across the consortium, and to provide the analytical baseline against which D7.2 and D7.3 will develop specific service offerings and business models.

8. Per-Country Market Impact

The following sections examine the market context in each of the seven consortium countries. Each section covers the national regulatory environment relevant to HOMEPOT, the vertical context in which the national demonstrator is positioned, and the exploitation pathways available to the consortium partners active in that country. The analysis is grounded in current, publicly available data sources cited in Section 12 and validated against the demonstrator activities documented in WP6.

8.1. Belgium

National regulatory context

Belgium was the first EU Member State to complete the transposition of the NIS2 Directive. The Belgian NIS2 law (Loi/Wet of 26 April 2024), accompanied by the implementing Royal Decree of 9 June 2024, entered into force on 18 October 2024. The Centre for Cybersecurity Belgium (CCB) was designated as the national cybersecurity authority and CSIRT. By late November 2025, approximately 1,500 essential entities and 2,500 important entities had registered with the CCB via the Safeonweb@Work portal. Registration for entities in scope was required by 18 March 2025, and the first conformity assessment deadline for essential entities fell on 18 April 2026, with full audit-readiness required by 18 April 2027.

Belgium is distinctive in the EU for tying NIS2 enforcement to an auditable national baseline, the CyberFundamentals (CyFun) framework, which is derived from NIST CSF, ISO 27001, and CIS Controls. Essential entities are subject to ex-ante supervision, and administrative fines can reach EUR 10 million or 2% of worldwide annual turnover, whichever is higher. Belgian NIS2 law also provides for personal liability of board members, including potential temporary suspension from management functions. This regulatory environment creates a structural demand for endpoint management platforms capable of demonstrating auditable compliance, jurisdictional data control, and traceable policy enforcement. HOMEPOT is aligned with each of these requirements by design.

Vertical context: renewable energy asset management

Belgium is one of the most digitalised renewable energy markets in Europe. Renewables accounted for approximately 46.8% of the country's electricity generation in 2021 and continue to grow. The updated Belgian National Energy and Climate Plan targets 15.5 GW of installed solar photovoltaic capacity by 2030, with Flanders alone targeting 13.2 GW. Long-term ambition extends to 33.6 GW of solar capacity by 2035. Offshore wind capacity is targeted at approximately 5.7 GW by 2030, with 2.26 GW already installed and a second offshore wind zone under construction. Belgium is a global leader in offshore wind and one of the signatories of the North Sea Ostend declaration for 120 GW of joint offshore capacity by 2030.

At the European level, the current NECP baseline puts the EU on track for approximately 650 GW of installed solar capacity and 450 GW of installed wind capacity by 2030. This distributed capacity is spread across tens of thousands of utility-scale sites and hundreds of thousands of commercial, industrial, and residential rooftops. Each site requires secure, remote, bi-directional communication for monitoring and control, and each falls within the tightening perimeter of the NIS2 essential-entity classification for the energy sector. The overlap between renewable energy asset digitalisation and endpoint management is direct.

Consortium partner positioning

The Belgian sub-consortium comprises three partners with distinct roles in the value chain.

3E, headquartered in Brussels, is a leading technology and SaaS company for the digitalisation of renewable energy assets. Its SynaptiQ platform, based on a physics-based digital twin architecture, currently manages approximately 25 GW of connected solar, wind, and battery storage assets across 160 countries. Its customer base includes major independent power producers and

operations-and-maintenance providers, including BayWa, Engie, EDP, Voltalia, and Eneco, together with more than 200 other industry participants. 3E's participation in HOMEPOT positions it to extend SynaptiQ's asset-management capabilities into the secure device-management layer, addressing the growing NIS2 compliance requirements for its customer base and supporting the operational management of the geographically distributed, heterogeneous device populations that characterise modern renewable energy portfolios. 3E's role as Task 7.1 leader further reinforces its position within the WP7 business model definition activities.

SIRRIS, the collective research centre of the Belgian technological industry, contributes expertise in cybersecurity, artificial intelligence, and machine learning applied to industrial device management. SIRRIS operates the EluciDATA Lab, its Data and Artificial Intelligence Competence Lab, established in 2009, and maintains an active portfolio of research and industrial collaboration in cybersecurity for manufacturing, including specific programmes targeting NIS2 and Cyber Resilience Act compliance for Belgian manufacturers and product developers. SIRRIS has an existing collaboration record with 3E on IoT and data analytics for renewable energy asset configuration, established through prior European research projects. Within HOMEPOT, SIRRIS supports both the Belgian demonstrator and the transfer of results to the broader Belgian industrial ecosystem, including through its role in the Brussels Initiative on Cybersecurity Innovation and the Flemish Industriepartnerschap.

Nokia Bell N.V. contributes domain solution provision, cloud secure access platform capabilities, software development, and use-case validation. Its participation in HOMEPOT is aligned with Nokia's Innovation Framework, which provides pathways from research outputs to internal incubation or external venture creation in domains adjacent to Nokia's core business. This positioning enables HOMEPOT-derived capabilities to be developed further beyond the project lifetime through Nokia's established innovation and commercialisation infrastructure.

Market impact and exploitation

The Belgian sub-consortium is well positioned to translate HOMEPOT outputs into measurable market impact across three vectors. First, 3E's exploitation of HOMEPOT extends its established SaaS asset management position into the security and device management dimensions required by NIS2 for its energy-sector customer base, both in Belgium and internationally. Second, SIRRIS provides a route for HOMEPOT results to reach the broader Belgian industrial ecosystem through its role as the country's technological research centre and its established dissemination and training programmes. Third, Nokia Bell N.V.'s participation opens pathways for further development and commercial exploitation of HOMEPOT outputs within Nokia's global innovation framework.

8.2. Czechia

National regulatory context

Czechia completed the transposition of the NIS2 Directive through the Cybersecurity Act (Act No. 264/2025 Coll.), which entered into force on 1 November 2025. The Act is administered by NÚKIB (National Cyber and Information Security Agency) and follows the NIS2 two-tier structure of essential and important entities. Regulated entities have 60 days from receiving their registration decision to self-identify with NÚKIB and a further one-year transition period to implement the required security controls. Administrative fines can reach 250 million CZK, and the Act extends beyond the NIS2 minimum in several respects: essential entities must report all incidents within their regulated ISMS

scope rather than only significant ones, the government has explicit powers to restrict insecure supply chain products and vendors, and regulated entities must appoint distinct cybersecurity manager, architect, and auditor roles.

The Critical Infrastructure Resilience Act (Act No. 266/2025 Coll.), transposing the EU CER Directive, entered into force on the same date, extending the resilience obligations for operators of critical infrastructure. The Czech government's "Country for the Future 2.0" national economic strategy, announced in February 2026, further prioritises digital transformation, AI adoption, and R&D expansion. Together, these developments establish a strong national demand for auditable endpoint management and secure device lifecycle handling in regulated environments.

Market context

The Czech ICT market was valued at approximately USD 22.5 billion in 2025 and is projected to reach USD 33.91 billion by 2031, representing a CAGR of 7.08% (Mordor Intelligence, 2026). Growth is driven by EU recovery funds, accelerated 5G deployment, and rising cybersecurity spend in anticipation of full NIS2 enforcement. Smart Factory and Industry 4.0 solutions are advancing faster than the overall ICT market, at a CAGR of 8.95% through 2031, and managed cloud services represent the fastest-growing service line. The government targets 100% online public-service availability and 80% cloud and AI adoption among firms by 2030.

Prague hosts the National Centre for Industry 4.0 alongside the national centres for Construction 4.0 and Transport 4.0, all coordinated through CIIRC CTU, reinforcing Czechia's established position in the European Industry 4.0 landscape. The Czech telecom market is developing IoT-oriented offerings alongside 5G rollout, with more than 93% 5G population coverage achieved by late 2024 and enterprise IoT connections contributing meaningfully to operator growth. The combination of regulatory pressure, industrial digitalisation momentum, and public sector demand aligns with the operational challenges HOMEPOT is designed to address.

Consortium partner positioning

The Czech sub-consortium consists of a single partner, EXPECT-IT s.r.o., which acts as Czech country coordinator and leads WP6 (Integration and Evaluation of the Demonstrators). EXPECT-IT participates in HOMEPOT on a fully self-funded basis, reflecting a direct commercial commitment to translating project results into market outputs.

EXPECT-IT's participation focuses on a recurring challenge in Czech industry: reducing operational cost when IT systems combine components from multiple manufacturers whose interfaces do not align, and clarifying supplier responsibility when problems arise across such heterogeneous stacks. The Czech contribution also emphasises standardisation across converged IT and IoT solutions, together with the promotion of open interfaces and open data approaches that reduce vendor lock-in, an aspect directly relevant in a market currently absorbing the churn dynamics identified in Section 4.5.

Within HOMEPOT, EXPECT-IT extends its existing GPC framework with new capabilities for monitoring and managing devices built on heterogeneous underlying architectures. Target application domains include smart city initiatives, security and surveillance system monitoring, and sensor-driven infrastructure for municipalities, schools, and private enterprises in Czechia. As WP6 leader, EXPECT-IT also holds a transversal role in the project, integrating the platform across all seven

national demonstrators and gaining direct visibility into the technical outputs that will be exploited domestically and in cross-border deployments.

Market impact and exploitation

The Czech sub-consortium's impact is concentrated along two vectors. The first is domestic: EXPECT-IT's extended GPC framework is positioned to serve the growing Czech demand for auditable, standards-aligned endpoint management under NIS2 and the Critical Infrastructure Resilience Act. The second is cross-border: the WP6 integration role provides EXPECT-IT with a strong position from which to engage with partner ecosystems in the other consortium countries, opening opportunities for joint integration and managed-service delivery beyond Czechia.

8.3. Germany

National regulatory context

Germany completed the transposition of the NIS2 Directive through the NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), which amends the BSI Act (BSIG). The Act was adopted by the Bundestag on 13 November 2025, approved by the Bundesrat on 21 November 2025, and entered into force on 6 December 2025. Germany did not adopt a standalone NIS2 law but instead layered the new obligations onto the pre-existing KRITIS framework administered by the BSI (Bundesamt für Sicherheit in der Informationstechnik).

The German implementation is one of the most stringent in the European Union in three respects. First, no transitional period was provided: obligations applied immediately from 6 December 2025. Second, the scope of regulated entities was expanded from approximately 4,500 under the previous framework to around 29,500 across 18 sectors, an expansion of over sixfold. Registration with the BSI is required by 6 March 2026 through a two-step process that combines the Mein Unternehmenskonto authentication layer with the BSI portal that went live on 6 January 2026. Third, personal liability for management bodies, including Geschäftsführer and Vorstand, is set out explicitly, with potential fines and temporary bans from management functions in addition to the corporate sanctions. Fines can reach EUR 10 million or 2% of global annual turnover for particularly important entities, and EUR 7 million or 1.4% for important entities.

The immediate applicability, the sixfold expansion of scope, and the personal management liability together create a strong and time-bound demand for auditable endpoint management platforms in Germany. Enforcement activity has already begun: the BSI issued formal notices in Q4 2025 to entities that had failed to register, prioritising the energy and digital infrastructure sectors.

Market context

Germany is the largest Enterprise Mobility Management market in continental Europe. National EMM revenues are projected to reach USD 10.6 billion by 2035, at a CAGR of approximately 22% (Meticulous Research, 2025). Demand is shaped by three factors that align closely with HOMEPOT's design principles.

The first is Industry 4.0. Germany's automotive and manufacturing sectors are the primary sources of enterprise device management demand, driven by the ongoing digitalisation of factories, logistics operations, and field service processes. This vertical is directly connected to the 54.1% CAGR for 5G endpoints in manufacturing identified in Section 3.4, and it favours platforms capable of managing heterogeneous mixes of IT, IoT, and interactive-UI devices under a common management plan.

The second is the German preference for GDPR-aligned, sovereignty-conscious deployment. Enterprise customers routinely require that management data be hosted within Germany or within the wider EU, and audit trails must be demonstrably compliant with national data protection expectations. This preference translates directly into a market advantage for platforms designed with European regulatory compliance as a starting point rather than a retrofit.

The third is banking and financial services. Regulated banks were early German adopters of EMM, and the introduction of DORA extends comparable requirements across a wider financial services perimeter. The sector represents a high-value entry point for auditable, control-heavy endpoint management offerings.

A distinctive feature of the German UEM competitive landscape is the presence of established regional challengers such as Matrix42 and Ivanti alongside the global incumbents identified in Section 4.2. This mixed structure indicates that there is room for differentiated European platforms in the German market, particularly those offering sovereignty-flexible deployment and vertical specialisation.

Consortium partner positioning

The German sub-consortium is represented by IOTIQ GmbH, a Leipzig-based SME and the WP7 leader. IOTIQ operates as a technology provider with an established position in mobile device management, targeting German-speaking enterprise and public-sector customers. Its participation in HOMEPOT is self-funded, reflecting direct commercial commitment to translating project outputs into market offerings.

IOTIQ's role in HOMEPOT is anchored by its WP7 leadership responsibility for the definition of new business models. This position aligns naturally with the strong German market context set out above, where NIS2 immediacy, Industry 4.0 demand, and GDPR-aligned procurement preferences together create an accessible and time-sensitive commercial opportunity. IOTIQ's WP7 leadership therefore places the project's business model definition activities in one of the most active endpoint management markets in Europe.

Market impact and exploitation

The German sub-consortium's impact operates on three vectors. First, the immediate NIS2 environment provides a near-term entry point for HOMEPOT-derived offerings, particularly among the approximately 25,000 newly regulated entities that must adapt their endpoint management practices from a standing start with no transition period. Second, the Industry 4.0 vertical provides a longer-term extension pathway across German manufacturing and adjacent industries, where heterogeneous device populations are a persistent operational challenge. Third, IOTIQ's WP7 leadership feeds directly into the D7.2 and D7.3 activities that will define the specific service offerings and business models through which the German market is addressed.

8.4. Korea

National regulatory context

South Korea maintains one of the most stringent data protection frameworks outside the European Union, centred on the Personal Information Protection Act (PIPA). PIPA was substantially amended in 2023, further updated through the Enforcement Decree effective 2 October 2025, and then subject to its most consequential rewrite in years, promulgated on 10 March 2026 and taking effect on 11 September 2026. The framework is administered by the Personal Information Protection Commission (PIPC).

The 2026 amendment introduces three changes that directly affect endpoint management demand. First, administrative fines can now reach 10% of a company's total revenue for high-severity violations, placing PIPA among the most consequential privacy regimes globally. Second, personal supervisory liability is placed on the CEO, who is designated as the ultimate person responsible for personal information protection. Third, the Chief Privacy Officer appointment must be approved by the Board of Directors and reported to PIPC for entities meeting size criteria, and ISMS-P (Personal Information and Information Security Management System) certification, previously voluntary, is now mandatory for private entities meeting specific thresholds.

Two supporting developments matter for the Korean market context. Data portability rights have applied since 13 March 2025, requiring controllers to implement mechanisms such as encrypted downloads or APIs. The PIPC granted the European Union an adequacy decision on 16 September 2025, allowing personal data to flow between Korea and EU countries without additional consent. This adequacy is directly relevant to HOMEPOT partners in Belgium, Czechia, Germany, Portugal, and the United Kingdom, as it lowers the friction of cross-border data flows involving Korean deployments.

The combined effect of the 2026 PIPA amendment is a substantial and time-bound increase in demand for auditable, governance-accountable endpoint management platforms among Korean businesses processing personal data at scale.

Market context

The global Location-Based Services (LBS) market, directly relevant to the Korean sub-consortium's mobility positioning, was valued at USD 61.9 billion in 2025, is estimated at USD 71.8 billion in 2026, and is projected to reach USD 467.2 billion by 2035 at a CAGR of 23.1% (Research Nester, 2025). The Asia-Pacific region is the fastest growing, with a projected CAGR of 23.8% over 2026 to 2035, driven by rapid urbanisation, high mobile adoption, and government spending on smart-city infrastructure. This dynamic aligns directly with the Korean sub-consortium's stated expansion pathway into Southeast Asia.

The adjacent smart mobility market was valued at approximately USD 59 billion in 2025 and is projected to grow to between USD 180 billion and USD 255 billion by 2033-2034, at a CAGR of 15.3% to 19.4% (Grand View Research, Fortune Business Insights). Within this market, IoT is the largest

technology segment, ride-sharing is the largest offering segment, and traffic management is the largest solution segment.

The Korean ride-hailing market is heavily consolidated. Kakao Mobility, through the Kakao T super-app, holds approximately 90% market share and operates a dispatch platform serving more than 250,000 registered taxi drivers. The Korean sub-consortium's demonstrator is positioned in an adjacent segment: business-to-business dispatch infrastructure serving regional taxi operators, corporate taxi companies, and individual taxi associations. This is a distinct part of the mobility stack, closer to fleet management and logistics than to consumer ride-hailing.

Korea's national digital infrastructure ambition provides a further contextual anchor. In June 2025, ETRI was selected by the Korean government to lead the development of a 6G-standard non-terrestrial network satellite-IoT communication system, in collaboration with Hanwha Systems, Korea Aerospace Industries, KT SAT, SK Telecom, and LG U+, with the objective of establishing a national satellite-IoT ecosystem by 2030. HOMEPOT's Korean sub-consortium is therefore embedded within a national digital infrastructure programme of significant strategic scale.

Consortium partner positioning

The Korean sub-consortium comprises three partners with complementary roles. **Essetel Co., Ltd.** operates the demonstrator deployment, a real-time location-based taxi dispatch control system serving more than 40 regions across South Korea, with a stated ambition to expand to more than 60 regions within two years and to explore international opportunities, particularly in Southeast Asia. **ETRI (Electronics and Telecommunications Research Institute)** acts as Korean country coordinator and leads WP4 (Data Analysis and Algorithms), bringing the country's leading government-affiliated research and technology organisation for electronics and telecommunications into the project. **Chungnam National University** contributes research and development capability.

Together, the three partners cover the Korean value chain from commercial deployment (Essetel) through research and technology transfer (ETRI) to academic research (Chungnam National University), providing a full pathway from HOMEPOT platform outputs to Korean market application.

Market impact and exploitation

The Korean sub-consortium's impact operates on three vectors. First, the PIPA 2026 amendment creates a near-term compliance-driven demand for endpoint management platforms among Korean businesses, particularly those handling personal data at scale in mobility, telecommunications, financial services, and public-sector contexts. HOMEPOT's design principles of auditability, governance accountability, and jurisdictional data control align directly with these requirements.

Second, the mobility demonstrator provides a validated entry point into the fast-growing Asia-Pacific LBS market, with Southeast Asia identified as the primary international expansion target. The 23.8% regional CAGR through 2035 sustains this pathway.

Third, ETRI's leadership of Korea's national satellite-IoT programme establishes a strategic alignment between HOMEPOT and Korea's future connected-device infrastructure. This positions the project's outputs to inform, and potentially contribute to, national-scale infrastructure work extending beyond the project lifetime.

8.5. Portugal

National regulatory context

Portugal completed the transposition of the NIS2 Directive through Decreto-Lei n.º 125/2025, published in the Diário da República on 4 December 2025 and entering into force on 3 April 2026, 120 days after publication. The decree establishes the new Regime Jurídico da Cibersegurança (RJC), which replaces the previous Lei 46/2018 and reinforces the Centro Nacional de Cibersegurança (CNCS) as the national cybersecurity authority. Portugal, like Germany and Czechia, did not meet the EU October 2024 transposition deadline. Regulamento n.º 756/2026, published on 22 June 2026, sets out the practical implementation rules, including the operation of the MyCiber electronic platform used for registration, compliance self-assessment, and CNCS communications.

The regulated entity population expanded from approximately 1,000 organisations under the previous framework to an estimated 7,000 to 9,000. Essential and important entities must appoint a cybersecurity officer and establish a permanent 24-hour contact point within 20 working days of entry into force. The National Reference Framework for Cybersecurity (QNRCS), based on the NIST Cybersecurity Framework 2.0, adds a new "Manage" function that reinforces the governance component of cybersecurity. After the regulatory framework is fully approved, essential, important, and relevant public entities have 24 months to adopt the new regime's standards.

Administrative fines can reach EUR 10 million or 2% of global annual turnover for essential entities, and EUR 7 million or 1.4% for important entities. Personal liability for members of management bodies is non-delegable. This combination of expanded scope, structured 24-month adoption horizon, and governance-level accountability creates a sustained national demand for auditable endpoint management platforms across Portuguese essential and important entities.

Market context

The Portuguese IoT market is projected to grow from its current baseline to approximately USD 14.75 billion by 2034, at a CAGR of 13.63% (IMARC Group, 2025). Growth is anchored in three coordinated national programmes: the National Digital Strategy adopted in 2024, which sets out frameworks for AI integration, data sharing, and sovereign cloud infrastructure; the Digital Agenda 2030, providing funding for rural connectivity and nationwide network enhancement; and the Portuguese Industry 4.0 Initiative, which provides EUR 200 million in grants and tax incentives for automation, IoT sensors, and digital skills development.

The Portuguese telecom sector is characterised by high fibre penetration, near-complete 5G population coverage, and substantial investment commitments. The Portuguese Infrastructure Ministry announced in November 2024 that the three major telecom operators (MEO, NOS, and Vodafone) would collectively invest approximately EUR 4.2 billion over five years in 5G networks, satellite communication systems, and fibre optic expansion. Portugal reached approximately 75% 5G population coverage by mid-2024, with a national target of 90% by 2027. The 5G Standalone (5G SA) network is now operational in Portugal, and Mobile Edge Computing solutions have been deployed in partnership with global cloud providers, enabling ultra-low-latency applications relevant to industrial IoT, autonomous systems, and real-time healthcare use cases. The Sines Data Centre and associated intercontinental subsea cable investments position Portugal as a Southern European connectivity hub.

The Portuguese consortium's positioning in HOMEPOT sits at the intersection of these three drivers: the regulatory expansion of NIS2-driven demand, the telecom-led acceleration of IoT and edge deployments, and the national ambition to build sovereign, secure digital infrastructure.

Consortium partner positioning

The Portuguese sub-consortium comprises three partners with complementary roles.

NOS Inovação contributes the industrial and telecom operator perspective, acting as use case provider and system integrator. NOS is one of Portugal's three main mobile network operators and was the first to launch a 5G Standalone network in the country, providing the operator infrastructure context for HOMEPOT's IoT and edge security work.

ISEP (Instituto Superior de Engenharia do Porto) acts as Portuguese country coordinator and leads WP8 (Dissemination and Exploitation). ISEP is one of Portugal's largest engineering schools and hosts the CISTER Research Centre in Real-Time and Embedded Computing Systems, which is among the leading European research units in real-time and embedded computing, cyber-physical systems, and embedded cybersecurity. This research depth provides the academic foundation for the Portuguese contribution and supports the transfer of HOMEPOT results to the broader Portuguese ecosystem through ISEP's established industry partnerships.

Adyta LDA contributes secure solutions provision in collaboration with ISEP and NOS Inovação, focused on IoT security within the Portuguese ecosystem.

Market impact and exploitation

The Portuguese sub-consortium's impact operates on three vectors. First, NIS2 transposition creates a structured near-term compliance demand for auditable, governance-aligned endpoint management platforms across the estimated 7,000 to 9,000 newly regulated Portuguese entities, with the 24-month adoption horizon establishing a defined market window.

Second, the telecom-led IoT and edge deployment trajectory creates a direct commercial context for NOS Inovação's HOMEPOT engagement. The scale of committed operator investment, together with the emergence of carrier-integrated UEM patterns identified in Section 4.5, supports the extension of the Portuguese demonstrator work into wider operator-delivered service offerings.

Third, ISEP's leadership of WP8, combined with the CISTER Research Centre's established position in embedded systems research, provides an academic and dissemination pathway that carries HOMEPOT outputs into the Portuguese research ecosystem and downstream to national startup and industrial adopters. This positioning is aligned with the National Digital Strategy's emphasis on sovereign digital infrastructure.

8.6. Türkiye

National regulatory context

Türkiye has substantially strengthened its cybersecurity and data protection framework in the period during which HOMEPOT has been active. Three developments define the current national context.

Cybersecurity Law No. 7545 (Siber Güvenlik Kanunu) was enacted by the Turkish Grand National Assembly on 12 March 2025 and published in the Official Gazette on 19 March 2025. The Law establishes a comprehensive national cybersecurity framework and creates the Cybersecurity Directorate (Siber Güvenlik Başkanlığı) as the primary regulatory and audit authority under Presidential Decree No. 177 (8 January 2025). The Law's scope covers public institutions, private legal entities, professional associations, and individuals engaged with information systems, networks, or critical infrastructure. Critical sectors including finance, healthcare, energy, and telecommunications are subject to stricter cybersecurity obligations, mandatory 24-hour incident reporting, and regular audits. Administrative fines for critical infrastructure operators can reach 1% of net sales in the previous calendar year. Secondary legislation and certification procedures are being developed within one year of the law's publication.

KVKK (Kişisel Verilerin Korunması Kanunu, Law No. 6698), the Turkish personal data protection framework enacted in 2016, underwent substantial amendments in 2024 and 2025 aligning it more closely with the EU GDPR. The Regulation on Procedures and Principles Regarding the Transfer of Personal Data Abroad, in force since 1 June 2024, established a three-tier structure for lawful international transfers. The amendments introduced mandatory Data Protection Officers for medium and large enterprises, a 72-hour breach notification requirement, and administrative fines that in 2026 range up to approximately TRY 17 million for data security failures. VERBIS registration remains the operational mechanism for data controllers.

The Regulation on Network and Information Security (amended May 2025) reinforces threat detection and 24-hour reporting obligations under the BTK (Information and Communication Technologies Authority). Together, these three frameworks create a substantial and time-bound compliance demand for auditable, governance-aligned endpoint management platforms across the Turkish public sector, financial services, energy, telecommunications, and manufacturing.

Market context

Türkiye is positioned as a digital interconnection bridge between Europe, the Middle East, and Asia. The 2025 Turkish public-investment programme allocated approximately USD 46.2 billion to public digital infrastructure, of which USD 16.3 billion is directed at communications infrastructure, sovereign cloud adoption, and fibre-to-the-home coverage. The National AI Strategy targets AI contributions equivalent to 5% of GDP and 50,000 new skilled jobs. Domestic hosting preference has become an explicit procurement priority for municipal and central-government agencies, driving migration from offshore data pools to Tier III and Tier IV Turkish data centres.

The Turkish data centre market reached 66 MW of installed IT load in 2025 and is projected to expand to 140 MW by 2030, at a CAGR of 16.23% (Mordor Intelligence, 2026). Connected-device volumes in Türkiye reached 18.8 billion in 2024, up 13% year-on-year. The national 5G rollout, accelerated by the ULAK-TURKSAT private-network agreement in March 2025, is expanding the connectivity foundation on which endpoint management operates. These national dynamics, combined with the global MDM/UEM market conditions established in Section 3, create a substantial market opportunity for a differentiated, sovereignty-flexible platform originating from the Turkish consortium.

Consortium partner positioning

The Turkish sub-consortium is the largest in HOMEPOT, with five partners covering UEM and operating system development, cybersecurity provision, system integration, and device manufacturing. The sub-consortium also holds the overall project coordination role.

ERSTE Software Limited is the overall HOMEPOT project coordinator and leads WP1 (Project Management) and WP3 (Design of Platform Architecture). ERSTE contributes UEM and operating system provision through its MobiVisor platform. Its established customer engagements, referenced in the project baseline, cover confectionery production and distribution, telecommunications cybersecurity, banking-grade UEM under stringent financial regulation, and social services data protection in a cross-border deployment. This customer base demonstrates cross-sector and cross-border applicability directly relevant to HOMEPOT's positioning.

Dakik Yazılım Teknolojileri leads WP5 (Platform Implementation) and contributes across the full project value chain, from requirements definition and architecture through implementation, demonstration, and exploitation. Dakik's positioning combines UEM expertise with cybersecurity depth, forming the technical core of the Turkish sub-consortium's joint exploitation pathway together with ERSTE Software.

KoçSistem leads T7.2 (Service Business Offerings). Founded in 1945 and part of Koç Holding, KoçSistem is one of Türkiye's largest IT services organisations, serving clients in more than 30 countries across banking, retail, energy, durable consumer goods, automotive, government, and insurance. It operates Türkiye's first Security Operation Centre and has built its recent commercial positioning around Cybersecurity Law No. 7545 compliance, bundling managed security services with colocation for regulated customers. This positioning aligns directly with the services-led differentiation trend identified in Section 4.5 and with the 27.3% CAGR services segment identified in Section 3.5.

BLC İletişim ve Güvenlik Sistemleri Ltd. contributes cybersecurity, cloud secure access infrastructure and platform provision, and leads the system integration and software testing task as well as the internal communication task. BLC's positioning around 5G core and edge platforms creates joint exploitation opportunities in vertical applications including Vehicle-to-Everything communications, port automation, and smart city deployments, aligned with Türkiye's active 5G and edge computing agenda.

Arçelik A.Ş. contributes as device manufacturer and use case provider. Arçelik is one of Türkiye's largest industrial companies by international footprint, with subsidiaries in 58 countries, 45 production facilities in 13 countries, and consolidated turnover of approximately EUR 10.7 billion in 2025. Its 22-brand portfolio includes Arçelik, Beko, Grundig, Hotpoint, Indesit, Blomberg, and Bauknecht, among others. Following the 2024 formation of Beko Europe through the merger with Whirlpool Corporation's European operations, the group holds the largest home appliances market share in Europe by production volume. Arçelik operates 28 R&D and Design Centres worldwide with more than 2,000 researchers and holds over 4,500 international patent applications. The company has established credentials in IoT security, including recognition as IoT Security Champion by the IoT Security Foundation and IoT Security Assured certification for connected appliances. Its participation as the only device manufacturer in the HOMEPOT consortium anchors the project's positioning around devices with dynamic and interactive user interfaces, including smart TVs, smart room applications, and connected appliances relevant to hospitality, healthcare, and education environments.

The Turkish sub-consortium benefits from the corporate proximity of KoçSistem and Arçelik, both part of the Koç Holding group, which creates a natural pathway for coordinated exploitation of HOMEPOT outputs across the group's IT services and device manufacturing operations.

Market impact and exploitation

The Turkish sub-consortium's impact operates on four vectors.

First, the domestic regulatory environment created by Cybersecurity Law No. 7545, the KVKK amendments, and the Network and Information Security regulation drives near-term, structured demand for auditable endpoint management platforms across Turkish critical infrastructure sectors, financial services, energy, telecommunications, and manufacturing. All five Turkish partners are positioned to serve this demand through their respective value chain roles.

Second, the sub-consortium's international footprint extends the addressable market well beyond Türkiye. KoçSistem's client base in more than 30 countries, Arçelik's presence in 58 countries, and ERSTE Software's cross-border customer engagements together create a distributed exploitation pathway that carries HOMEPOT outputs into European, Central Asian, Middle Eastern, and North African markets.

Third, Türkiye's positioning as a digital interconnection bridge, combined with the sovereignty-flexible design of HOMEPOT and the sub-consortium's cybersecurity depth, creates a distinctive value proposition for markets in which European regulatory alignment and regional cultural or language proximity both matter.

Fourth, the project coordination role held by ERSTE Software provides the Turkish sub-consortium with direct visibility into the strategic direction of HOMEPOT as a whole, supporting the alignment of Turkish exploitation activities with the broader project trajectory. Public-private collaboration between the Turkish partners and national institutions is expected to inform continued regulatory and policy development in cybersecurity and endpoint management.

8.7. United Kingdom

National regulatory context

The United Kingdom's cybersecurity legislative framework is currently in transition. The **Cyber Security and Resilience (Network and Information Systems) Bill** was introduced to Parliament on 12 November 2025 and had passed its second reading and committee stage by early 2026. Report stage and third reading were scheduled for 10 June 2026, with Royal Assent anticipated during the second half of 2026. The Bill reforms and extends the existing Network and Information Systems Regulations 2018, the UK's transposition of the original 2016 NIS Directive, which had been widely regarded as insufficient in light of the evolving cyber threat landscape.

The Bill expands the regulatory scope in several respects. It brings Managed Service Providers into scope for the first time, recognising their access to essential-service infrastructure, and designates standalone data centres as essential services (thresholds of 1 MW rated IT load for standalone facilities and 10 MW for enterprise data centres). It broadens incident reporting requirements,

extends supply-chain security duties, and provides regulators with new powers to designate critical suppliers, bringing them directly within scope even where they would not otherwise qualify. Financial penalties are set on a two-band structure: up to GBP 17 million or 4% of global annual turnover for the most serious breaches, and up to GBP 10 million or 2% for less serious breaches. Enforcement, supervision, and technical guidance are led by the National Cyber Security Centre (NCSC) in coordination with sector-specific competent authorities.

The Bill's scope is notably narrower than the EU NIS2 Directive in one respect relevant to HOMEPOT's UK positioning. Manufacturing, retail, and food service sectors are not directly regulated by the Bill, although the government retains power to add sectors later. Nevertheless, the wider regulatory environment, including UK GDPR, the Data Protection Act 2018, and the Payment Card Industry Data Security Standard (PCI DSS), continues to impose substantial compliance obligations on any UK organisation processing personal or payment data at scale, including hospitality and food service operators.

The urgency of the UK cyber environment is reflected in the current threat data. NCSC managed 429 cyber incidents in the year to September 2025, of which 204 were classified as nationally significant, more than double the 89 recorded in the previous year. An independent report found that 95% of UK Critical National Infrastructure organisations experienced a data breach in 2024. Cyber-attacks are estimated to cost UK businesses approximately GBP 14.7 billion each year, equivalent to 0.5% of UK GDP. High-profile 2025 attacks against major UK retailers and manufacturers reinforced board-level attention to cyber governance. In October 2025 the UK government wrote directly to the top 350 UK businesses, reinforcing the importance of board-level cyber oversight and referencing the NCSC Cyber Assessment Framework and the Cyber Governance Code of Practice.

Market context

The UK hospitality and food service sector, the vertical in which HOMEPOT's UK demonstrator is positioned, is one of the largest and most digitally active service sectors in the UK economy. Turnover for restaurants, pubs, and related food service operations exceeded GBP 147 billion in mid-2025 and continues to grow. Inbound tourism is forecast to grow by 32% in value between 2024 and 2030, adding an estimated GBP 9.4 billion to the sector.

Technology investment in the sector has accelerated markedly. UK restaurants allocated approximately 9% of total sales to technology by 2022, up from below 2% pre-pandemic. Recent industry research indicates that 85% of UK restaurant leaders planned new technology investments for 2025, and approximately half of UK restaurant operators plan Point-of-Sale system upgrades in 2026. The UK POS software market is on track to reach USD 1.49 billion by 2030 at a compound annual growth rate of 9.4%, with the restaurant-specific segment growing faster at a CAGR of 12.8% through 2033. Hospitality is the primary driver of the UK POS market, ahead of retail and healthcare.

The device fleet operated by a modern UK restaurant is heterogeneous by design. Front-of-house Point-of-Sale terminals, self-service kiosks, tableside ordering tablets, kitchen display systems, back-of-house inventory management devices, delivery driver tablets, and increasingly IoT-enabled kitchen equipment for cold-chain and food safety monitoring all coexist within a single site. Multi-site operations extend this heterogeneity across geographically distributed premises. Integration with delivery platforms including Deliveroo, Just Eat, and Uber Eats, compliance with HMRC Making Tax Digital, tracking of the 14 required allergens, and PCI DSS payment security compliance together

create a complex operational environment that is difficult to manage with fragmented, single-vendor tooling.

The sector's cyber exposure has grown in step with its digital adoption. Ransomware attacks have forced UK restaurant chains to shut down online ordering channels, and back-end POS and ordering portals are frequently targeted. Sector commentators observe that restaurants are increasingly turning to managed security providers rather than attempting to handle cybersecurity internally. This trend aligns directly with the services-led differentiation pattern identified in Section 4.5 and the 27.3% CAGR services segment identified in Section 3.5.

Consortium partner positioning

The UK sub-consortium comprises three partners covering commercial deployment, application and technology provision, and academic research. Country coordination is provided by GetFudo, which delivers the UK demonstrator in the food service vertical, focused on managing heterogeneous device fleets across restaurant environments, including Point-of-Sale terminals, kiosks, kitchen systems, and delivery tablets. Dealdio Limited contributes application development and technology provision, with particular strengths in loyalty platform integration that create cross-consortium synergy opportunities with the Turkish device manufacturing and MDM partners. Brunel University London leads WP2 (Platform and Demonstrator Requirement Definitions) and contributes methodological depth in modelling, simulation, and Verification, Validation, and Uncertainty Quantification. The three partners together provide a self-contained UK exploitation pathway spanning commercial deployment, product technology, and academic validation.

Market impact and exploitation

The UK sub-consortium's impact operates on three vectors. First, the size and technology momentum of the UK hospitality and food service market create a substantial vertical opportunity for HOMEPOT-derived offerings. The heterogeneous device fleets characteristic of modern multi-site food service operations are precisely the deployment pattern that HOMEPOT is designed to address, and the sector's active investment in technology upgrades provides a receptive procurement environment.

Second, the elevated UK cyber threat level, the pending strengthening of regulatory obligations through the CS&R Bill, and the sector's own recognition that managed security services are increasingly necessary create a pull for auditable, professionally managed endpoint management platforms. HOMEPOT's positioning around vendor-independent device pools and open APIs is directly relevant to operators seeking to move beyond fragmented single-vendor tooling.

Third, the UK sub-consortium provides HOMEPOT with a distinctive vertical demonstration, one of the few in the consortium that combines a high-frequency consumer-facing operational environment with the full heterogeneity of interactive-UI devices that the platform is designed to manage. This anchoring in a consumer-scale operational context complements the industrial, telecom, and public-sector demonstrator contexts delivered by other national sub-consortia.

9. Market Impact Assessment

Section 9 consolidates the market analysis presented in Sections 3 to 8 into a structured assessment of the impact HOMEPOT is expected to deliver. The assessment is organised across three dimensions: quantitative indicators drawn from the project's KPIs, qualitative impact across positioning and ecosystem effects, and societal and sustainability impact aligned with European and national policy priorities. The assessment reflects the CR3 baseline and is intended to be revisited as WP7 progresses through D7.2 and D7.3.

9.1. Quantitative Indicators

HOMEPOT's measurable market impact will be tracked through the project's KPI framework, which was defined in the Full Project Proposal and refined through the change requests. Five headline KPIs are relevant to the commercial positioning developed in this deliverable.

Policy implementation success rate across heterogeneous devices and operating systems. The target of at least 95% success in applying management policies across the range of devices supported by the platform is central to HOMEPOT's positioning as a universal management platform. Commercially, this KPI supports the vendor-independence claim examined in Sections 4 and 7, and underpins the platform's ability to serve customers operating mixed device fleets without single-vendor lock-in.

Reduction in security incidents. The target of a 20% reduction in security incidents in HOMEPOT-managed environments compared to fragmented management baselines supports the platform's positioning within the NIS2, DORA, CS&R Bill, and equivalent national regulatory frameworks examined in Section 8. Demonstrable incident reduction is a direct commercial argument in the current market phase, where the churn dynamic identified in Section 4.5 has increased enterprise willingness to consider differentiated alternatives.

Reduction in manual configuration effort during device transitions. The target of 80% reduction in manual effort is directly relevant to the services segment of the market, which is growing at 27.3% CAGR (Section 3.5) and is constrained by the global shortage of in-house cybersecurity and IT operations expertise. Reducing the manual effort associated with onboarding, provisioning, and reconfiguration is a foundational condition for managed-service-based commercial offerings, which will be developed in D7.2.

User satisfaction improvement for adaptive management features. Measured through structured questionnaires, this KPI supports the Digital Employee Experience driver examined in Section 3.6 and provides evidence for HOMEPOT's positioning around interactive-UI device management, which distinguishes the platform from sensor-focused IoT platforms and from single-ecosystem UEM suites.

Privacy and ethical AI mechanisms implemented within the first 24 months. The delivery of privacy-aware and ethically designed AI mechanisms is directly connected to the EU AI Act, GDPR, KVKK, PIPA, and UK GDPR obligations examined in Section 8. As a KPI, this is both a technical deliverable and a commercial argument, positioning HOMEPOT to meet procurement requirements that are increasingly enforced by European and equivalent national buyers.

Each of these KPIs translates into a commercial argument that D7.2 and D7.3 will develop into concrete service offering and business model claims. The consolidated KPI table maintained under WP1 provides the reference figures against which performance will be measured.

9.2. Qualitative Impact

Beyond the KPIs, HOMEPOT is expected to deliver five qualitative impacts on the consortium's competitive positioning and on the wider market environment.

Regulatory alignment. The project's platform is designed to support compliance with NIS2 (Belgium, Czechia, Germany, Portugal), the CS&R Bill (United Kingdom, once enacted), DORA (all EU consortium countries), Turkish Cybersecurity Law No. 7545 and KVKK (Türkiye), and PIPA (Korea). This alignment positions the consortium partners ahead of the enforcement curve in each national context, converting compliance obligation into a commercial argument.

Vertical extensibility. The seven national demonstrators cover renewable energy, industrial IT integration, cross-vertical enterprise UEM, mobility, telecom and IoT, consumer electronics and critical infrastructure, and hospitality. Each demonstrator both validates the platform in a specific vertical and creates a credible reference for expansion into adjacent verticals, particularly healthcare, education, and smart city deployments referenced by multiple partners.

Partner brand and positioning. Each commercial partner acquires differentiated positioning that would be difficult to achieve individually. The academic and research partners strengthen their positioning in cybersecurity, embedded systems, and cyber-physical systems research at both national and European levels. The industrial and SME partners acquire a validated, referenceable platform on which to build their post-project commercial offerings.

Contribution to European technological sovereignty. HOMEPOT contributes to the European ambition of reducing dependence on non-European UEM platforms. Sovereignty-flexible deployment, alignment with European regulatory frameworks, and a value chain that is fully covered by European and allied consortium partners are direct contributions to this ambition. In the current market phase, characterised by the pricing disruption following the Broadcom acquisition of VMware and by rising enterprise sensitivity to jurisdictional data control, this positioning has commercial value that goes beyond policy alignment.

Cross-border partnership network. The consortium establishes a referenceable cross-border deployment network spanning Belgium, Czechia, Germany, Korea, Portugal, Türkiye, and the United Kingdom. Single-vendor incumbents cannot easily replicate this pattern, and the network itself becomes an exploitation asset that supports partner-led expansion into markets where consortium members have established commercial presence.

9.3. Societal and Sustainability Impact

HOMEPOT's societal and sustainability impact is aligned with the objectives of the European Green Deal, the EU 2030 Digital Compass, and the United Nations Sustainable Development Goals. Five points of impact are identified.

Regulatory compliance enablement for essential and important entities. By supporting NIS2, DORA, and equivalent national frameworks, HOMEPOT contributes to the wider objective of raising the

cybersecurity resilience of European critical infrastructure operators and digital service providers. Given the current threat data (NCSC recording 204 nationally significant UK cyber incidents in 2024-25, a majority of European CNI operators experiencing at least one breach), the contribution is directly relevant to public safety and operational continuity.

Renewable energy integration. The Belgian demonstrator supports the secure operation and management of renewable energy assets at the scale required by EU 2030 targets and the updated Belgian NECP. This aligns with UN Sustainable Development Goal 7 (Affordable and Clean Energy) and Goal 13 (Climate Action).

Public safety and mobility. The Korean demonstrator enhances the safety of location-based mobility services through secure device management and integration with guardian access mechanisms. The wider mobility application area, including in-vehicle systems and dispatch infrastructure, contributes to Goal 11 (Sustainable Cities and Communities).

Operational reliability in consumer-facing services. The UK food service demonstrator supports the operational continuity of hospitality and food service operations that are increasingly exposed to cyber risk. Given the sector's employment scale and the recent losses of nearly 60,000 UK jobs in the year to September 2025, operational resilience in consumer-facing sectors carries direct social impact.

Digital sovereignty and skills development. The consortium's academic partners, including SIRRIS in Belgium, ISEP in Portugal, Brunel University London in the United Kingdom, ETRI and Chungnam National University in Korea, contribute to the development of specialised skills in cybersecurity, embedded systems, and platform engineering that address the wider European and national skills gaps in these areas. This is aligned with the EU 2030 Digital Compass target of 20 million ICT specialists in the European Union.

The consolidated market impact assessment supports the direct hand-off to D7.2 and D7.3, in which the qualitative and quantitative indicators identified here will be translated into concrete service offerings and validated business models.

10. Risks, Barriers, and Mitigation

Any market baseline needs to be read alongside a clear-eyed view of the risks that could constrain HOMEPOT's ability to translate the opportunity into commercial impact. This section identifies the principal risks and barriers relevant to the market and exploitation dimensions of the project. It does not duplicate the technical or project management risk registers maintained under WP1, which cover delivery-side risks such as staffing, integration, and demonstrator timelines. The focus here is on market, competitive, regulatory, and exploitation risks that affect the WP7 analysis directly.

Ten risks are identified. For each, the description is followed by the mitigation approach available to the consortium.

Incumbent vendor dominance. Microsoft, VMware, IBM, JAMF, and BlackBerry collectively hold 45% to 50% of the MDM/UEM market, with deep enterprise penetration and substantial customer inertia. Direct competition in the incumbents' core segments is not commercially viable for a new platform. HOMEPOT's differentiated positioning around heterogeneity, vendor independence, vertical depth,

and sovereignty flexibility (Sections 4.6 and 7.2) is the mitigation. The project does not attempt to displace incumbents in their established segments but targets the gap areas that they address unevenly.

Slow procurement cycles in regulated and public sectors. Regulated verticals including energy, healthcare, financial services, and public administration typically operate procurement cycles measured in years rather than months. Long sales cycles can delay revenue capture. Early engagement through the demonstrator programme, pilot pathways delivered through existing partner customers, and managed-service entry routes that lower the initial commitment threshold are the principal mitigations.

Carrier bundling and telecom-integrated UEM offerings. Telecommunications operators including Verizon, AT&T, and equivalents in HOMEPOT's target markets are increasingly bundling MDM into 5G data plans, providing security enforcement at the network-slice level. This dynamic can reduce the addressable market for standalone UEM offerings. NOS Inovação's participation in the Portuguese sub-consortium provides a direct route to engage constructively with this trend rather than compete against it. HOMEPOT can be positioned as the platform that telecom operators integrate, rather than as a competing product.

Standards fragmentation across device management interfaces. The absence of common policy and device management standards across manufacturers has been one of the persistent obstacles to unified endpoint management. This limits the pace at which any new platform can extend coverage across the device landscape. HOMEPOT contributes to standardisation through its abstract policy mediator approach and through the consortium's participation in the wider standards ecosystem, coordinated under WP8 and D8.3.

Evolving cybersecurity threat landscape. The current threat data (an increase in nationally significant UK cyber incidents from 89 to 204 in a single year, 95% of UK Critical National Infrastructure organisations experiencing a data breach in 2024, PIPA and NIS2 penalty frameworks scaled to reflect the seriousness of contemporary risks) signals a threat landscape evolving faster than platform release cadences. Continuous security monitoring, alignment with NIS2 and equivalent frameworks, and participation in cyber threat intelligence sharing are the operational mitigations. The consortium's cybersecurity specialists (BLC, Adyta, SIRRIS) provide the technical foundation.

Post-quantum cryptographic transition. Following the standardisation of post-quantum cryptography by NIST (FIPS 203, 204, 205), enterprise customers are beginning to require demonstrable cryptographic agility from platform vendors. Platforms that cannot adapt are exposed to obsolescence risk over a multi-year horizon. HOMEPOT's policy mediator architecture and the cybersecurity expertise represented in the consortium support cryptographic agility. The project positions itself to inform this transition rather than to be caught by it.

Consortium volatility and partner changes. The history of Change Requests 1, 2, and 3 during the project's first eighteen months has shown that consortium composition and scope can change materially in response to external circumstances. Further changes are possible over the remaining project period and beyond. The modular design of both the platform and the exploitation strategy is the mitigation. The value chain analysis in Section 5 was structured to remain valid under moderate consortium change, and partner-level exploitation pathways are designed to be independently viable.

Market timing risk. Consolidation in the UEM market could reduce the window for differentiated challengers. If the current pricing disruption around Broadcom's VMware acquisition is resolved through customer retention concessions, the pool of active buyers considering alternatives could shrink. Pre-commercial engagements through the demonstrator programme, combined with alignment to the still-tightening regulatory environment, are the mitigation. Regulatory pressure operates on a slower and more predictable clock than pricing dynamics and provides a more stable foundation for HOMEPOT's market entry.

Regulatory divergence across HOMEPOT's target markets. The seven national regulatory frameworks covered in Section 8 share broad principles but differ meaningfully in the specific compliance mechanisms, penalty structures, and personal liability provisions. A single platform configuration is unlikely to satisfy all frameworks without adaptation. Configurable compliance profiles within the platform are the technical mitigation. Commercially, the diversity of the consortium's national coverage is itself an asset, as it exposes the platform to the range of variation early in its development.

Cost competitiveness against hyperscaler bundles. Microsoft, Google, and Amazon each bundle UEM or UEM-adjacent capabilities into their cloud subscription offerings. For customers already committed to a single hyperscaler ecosystem, the marginal cost of adding management capability from the same vendor is low. HOMEPOT's mitigation is to focus on scenarios where hyperscaler bundling does not extend effectively: heterogeneous multi-vendor deployments, sovereignty-sensitive environments where the choice of underlying cloud is constrained, and rugged IoT deployments where hyperscaler agents are ill-suited to the resource envelope of the target devices.

Two general observations apply across the risk register.

First, the risks are not independent. A slower NIS2 enforcement pattern in a given country would extend procurement cycles and reduce pricing pressure on customers currently affected by the Broadcom disruption. Conversely, faster regulatory enforcement compresses procurement cycles and enlarges the addressable pool of active buyers. HOMEPOT's market timing is therefore linked to the enforcement cadence of the regulatory frameworks examined in Section 8. This linkage argues for maintaining active alignment between technical delivery and regulatory implementation timelines through the remainder of the project.

Second, the identified risks are individually manageable within the CR3 baseline. None of the risks identified in this section is judged to be fundamentally destabilising, and the mitigation approaches available to the consortium are consistent with the exploitation pathways developed in T8.2 and to be further developed in D7.2 and D7.3. Continuous review of the risk register, aligned with the WP1 project risk log, is expected as WP7 progresses.

11. Conclusion and Outlook

HOMEPOT is being developed at a moment when the market it targets is expanding rapidly and reshaping itself in ways that align closely with the platform's design principles. The global Mobile Device Management market, valued at approximately USD 11 billion in 2026, is projected to more than double by 2030 and to exceed USD 30 billion by 2031, at a compound annual growth rate in the range of 18.5% to 24.5%. This growth is not incidental. It is driven by the convergence of MDM,

desktop management, and IoT management under Zero Trust architectures; by the transition from predictive to autonomous, or agentic, AI in endpoint security; by the surge in 5G-connected industrial and rugged IoT endpoints; and by the emergence of Digital Employee Experience as a serious competitive differentiator. Each of these drivers reflects a market that is moving toward the kind of platform HOMEPOT is being built to deliver.

The competitive picture is also favourable to a differentiated entrant. Five vendors hold approximately half of MDM/UEM revenue, and the remaining half is contested by regional players, vertical specialists, and open-source alternatives. Broadcom's pricing changes following the VMware acquisition have created active customer churn, enterprises are demanding cryptographic agility and sovereignty flexibility ahead of the post-quantum transition, and a set of persistent gap areas including rugged IoT management remain underserved by incumbent platforms. Innovation in the market has moved past feature parity. Services-led differentiation, anchored in cryptographic agility, API openness, and sovereignty flexibility, is now the primary determinant of customer retention. HOMEPOT is positioned along each of these dimensions by design rather than by retrofit.

The consortium's national coverage extends this positioning across seven distinct market and regulatory contexts. Belgium's early NIS2 transposition and the concentration of renewable energy assets provide the setting for 3E, SIRRIS, and Nokia Bell N.V. Czechia's Cybersecurity Act and Critical Infrastructure Resilience Act, alongside its Industry 4.0 momentum, define the context for EXPECT-IT. Germany's stringent NIS2 implementation, the largest continental European EMM market, and IOTIQ's WP7 leadership place the business model definition activities in a demanding and time-sensitive environment. Korea's PIPA amendments, the growth of location-based services, and ETRI's national satellite-IoT programme frame the Korean sub-consortium's positioning. Portugal's telecom-led IoT market and CISTER's research depth support the Portuguese contribution. Türkiye's Cybersecurity Law No. 7545, KVKK amendments, national digital infrastructure programme, and five-partner sub-consortium under ERSTE Software's project coordination provide the largest single national footprint in the consortium. The United Kingdom's transitional regulatory framework, high-value hospitality sector, and elevated cyber threat level define the context for the UK sub-consortium. Each demonstrator provides both technical validation and a credible entry point into a vertical or regional market.

The remainder of Work Package 7 will translate this market baseline into commercial substance. D7.2, led by KoçSistem, will define the specific service offerings through which HOMEPOT capabilities are brought to market. D7.3, led by IOTIQ, will validate the business models supporting those offerings, ensuring that the value chain positions identified in Section 5 are reflected in commercially viable exploitation structures. Both deliverables will draw on the market baseline established here and will remain aligned with the T8.2 Exploitation Plan under WP8, which addresses partner-level exploitation and Key Exploitable Results in parallel with the WP7 activity. The D8.1 Dissemination Plan and the D8.3 Standardisation Documentation will support the wider communication and standards positioning necessary to establish HOMEPOT's presence in the market.

Three points close this deliverable.

First, the market baseline established in D7.1 is intended to be revisited rather than fixed. The MDM and UEM market is moving rapidly, regulatory frameworks are entering force across the consortium's national footprint on staggered timelines, and the competitive landscape is shifting in response to both pricing dynamics and the post-quantum transition. The analysis presented here reflects the position at the point of submission and will be refreshed as necessary in subsequent WP7 outputs.

Second, the market opportunity is real but conditional. The favourable dynamics identified in this deliverable will translate into commercial impact for HOMEPOT partners only if the platform is delivered on time, at quality, and with the differentiation claimed here. The alignment between market signals and the project's technical roadmap is close, but the alignment must be actively maintained. The consortium's coordination structures under WP1, the continued integration progress under WP6, and the exploitation planning under WP8 are the mechanisms through which that alignment is preserved.

Third, HOMEPOT's positioning is credible on the evidence assembled in this deliverable. The market is large and growing. The competitive landscape has open gaps that match the platform's design. The regulatory environment across the consortium's national footprint favours sovereignty-flexible, auditable, jurisdictionally aware platforms. The consortium covers the value chain from academic research to end-user deployment across seven countries and nineteen partners. On this baseline, D7.2 and D7.3 can proceed to develop the service offerings and business models that will translate the market opportunity into partner-level exploitation.

References

[1] Mordor Intelligence, Mobile Device Management Market — Size, Share, and Trends Analysis, 2026–2031, Hyderabad, India, 2026. [Online]. Available: https://www.mordorintelligence.com/industry-reports/mobile-device-management-market

[2] Grand View Research, Mobile Device Management Market Size, Share and Trends Analysis Report by Component, Deployment, Organization Size, Vertical, and Region, 2025–2030, San Francisco, CA, USA, 2025. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/mobile-device-management-market

[3] The Insight Partners, Mobile Device Management Market — Global Outlook to 2031, New York, NY, USA, Jan. 2025.

[4] Strategic Market Research, Global Mobile Device Management Market Analysis: Zero Trust and Cloud Deployment, Maharashtra, India, 2024.

[5] Fortune Business Insights, Enterprise Mobility Management Market Report, 2026–2034, Pune, India, 2026.

[6] Meticulous Research, Germany Enterprise Mobility Management Market — Forecast to 2035, Pune, India, 2025.

[7] MarketsandMarkets, Mobile Device Management Market — Global Forecast to 2027, Rep. MD-MD-5562389, Pune, India, 2023.

[8] Omdia, Cellular IoT Connections Forecast to Reach 5.9 Billion by 2035, London, U.K., Jun. 2026. [Online]. Available: https://omdia.tech.informa.com

[9] IoT Analytics, Global Number of Connected IoT Devices — Annual Update, Hamburg, Germany, 2025. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[10] Transforma Insights, IoT Market Forecast and Highlights, Kimberley, U.K., 2025. [Online]. Available: https://transformainsights.com/research/forecast/highlights

[11] Research Nester, IoT Solutions and Services Market Report, 2025–2035, Rep. 8100, New Delhi, India, 2025. [Online]. Available: https://www.researchnester.com/reports/iot-solutions-and-services-market/8100

[12] ABI Research, 5G Industrial IoT and Endpoint Management, Oyster Bay, NY, USA, 2025.

[13] IMARC Group, Portugal IoT Market Report, 2025–2034, Noida, India, 2025.

[14] Mordor Intelligence, Turkey Data Center Market, 2025–2030, Hyderabad, India, 2026.

[15] Mordor Intelligence, Czech Republic ICT Market, 2025–2031, Hyderabad, India, 2026.

[16] Research Nester, Location-Based Services Market — Global Outlook 2025–2035, New Delhi, India, 2025.

[17] Grand View Research, Smart Mobility Market Size, Share and Trends Analysis Report, San Francisco, CA, USA, 2025.

[18] Fortune Business Insights, Smart Mobility Market Report, Pune, India, 2025.

[19] Research and Markets, China Mobile Device Management Market Forecast, Dublin, Ireland, 2024.

[20] Statista, South Korea Ride-Hailing Market: Kakao Mobility Market Share, Hamburg, Germany, 2026. [Online]. Available: https://www.statista.com

[21] IndustryARC, Healthcare Mobile Device Management Market Report, Hyderabad, India, 2024.

[22] Technavio, Education MDM Market Report, London, U.K., 2025.

[23] McKinsey & Company, Agentic AI in Cybersecurity, New York, NY, USA, 2025.

[24] National Cyber Security Centre, NCSC Annual Review 2025, London, U.K., Oct. 2025. [Online]. Available: https://www.ncsc.gov.uk/collection/annual-review-2025

[25] European Parliament and Council, "Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)," Off. J. Eur. Union, vol. L 333, pp. 80–152, Dec. 2022.

[26] European Parliament and Council, "Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA)," Off. J. Eur. Union, vol. L 333, pp. 1–79, Dec. 2022.

[27] European Parliament and Council, "Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)," Off. J. Eur. Union, series L, Nov. 2024.

[28] European Parliament and Council, "Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act)," Off. J. Eur. Union, series L, Jul. 2024.

[29] European Parliament and Council, "Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR)," Off. J. Eur. Union, vol. L 119, pp. 1–88, May 2016.

[30] European Commission, "Commission Implementing Decision on the adequate protection of personal data by the Republic of Korea," Brussels, Belgium, Sep. 2025.

[31] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS Pub. 203, Gaithersburg, MD, USA, Aug. 2024.

[32] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," FIPS Pub. 204, Gaithersburg, MD, USA, Aug. 2024.

[33] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard," FIPS Pub. 205, Gaithersburg, MD, USA, Aug. 2024.

[34] Belgium, "Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique", Moniteur Belge, May 2024.

[35] Belgium, "Arrêté royal du 9 juin 2024 portant exécution de la loi du 26 avril 2024," Moniteur Belge, Jun. 2024.

[36] Centre for Cybersecurity Belgium (CCB), CyberFundamentals Framework — Reference Guide, Brussels, Belgium, 2024. [Online]. Available: https://ccb.belgium.be/en/cyberfundamentals-framework

[37] Czech Republic, "Zákon č. 264/2025 Sb. o kybernetické bezpečnosti," Sbírka zákonů, Aug. 2025.

[38] Czech Republic, "Zákon č. 266/2025 Sb. o kritické infrastruktuře," Sbírka zákonů, Aug. 2025.

[39] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Implementation Guidance for the Cybersecurity Act, Brno, Czech Republic, 2025. [Online]. Available: https://nukib.gov.cz

[40] Germany, "NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)," Bundesgesetzblatt, Teil I, Dec. 2025.

[41] Bundesamt für Sicherheit in der Informationstechnik (BSI), NIS-2 Registration Portal - User Guide, Bonn, Germany, 2026. [Online]. Available: https://www.bsi.bund.de

[42] Republic of Korea, Personal Information Protection Act, Act No. 10465, as amended through 2026, Seoul, Republic of Korea.

[43] Personal Information Protection Commission (PIPC), Enforcement Decree and Guidelines on Cross-Border Personal Data Transfer, Seoul, Republic of Korea, 2025. [Online]. Available: https://www.pipc.go.kr

[44] Electronics and Telecommunications Research Institute (ETRI), "ETRI-led consortium selected for 6G-standard NTN low-orbit satellite-IoT communication system development," Press Release, Daejeon, Republic of Korea, Jun. 2025. [Online]. Available: https://www.etri.re.kr

[45] Portugal, "Decreto-Lei n.º 125/2025 — Regime Jurídico da Cibersegurança," Diário da República, Série I, Dec. 2025.

[46] Portugal, "Regulamento n.º 756/2026," Diário da República, Série II, Jun. 2026.

[47] Centro Nacional de Cibersegurança (CNCS), National Reference Framework for Cybersecurity (QNRCS), Lisbon, Portugal, 2025. [Online]. Available: https://www.cncs.gov.pt

[48] Republic of Türkiye, "Siber Güvenlik Kanunu (Cybersecurity Law) No. 7545," Resmi Gazete, no. 32846, Mar. 2025.

[49] Republic of Türkiye, "Cumhurbaşkanlığı Kararnamesi No. 177 — Establishment of the Cybersecurity Directorate," Resmi Gazete, Jan. 2025.

[50] Republic of Türkiye, Kişisel Verilerin Korunması Kanunu (KVKK), Law No. 6698, as amended through 2024–2025.

[51] Kişisel Verileri Koruma Kurumu, Guide on the Transfer of Personal Data Abroad, Ankara, Türkiye, Jan. 2025. [Online]. Available: https://www.kvkk.gov.tr

[52] United Kingdom, The Network and Information Systems Regulations 2018, Stat. Instr. No. 506, London, U.K., 2018.

[53] United Kingdom Parliament, Cyber Security and Resilience (Network and Information Systems) Bill, HC Bill 175, London, U.K., Nov. 2025. [Online]. Available: https://bills.parliament.uk

[54] UK Department for Science, Innovation and Technology, Cyber Security and Resilience Bill Policy Statement, London, U.K., Apr. 2025. [Online]. Available: https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

[55] United Kingdom, Data Protection Act 2018, London, U.K., 2018.