Europe IoT Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Europe IoT Security Market Analysis

The Europe IoT Security market size is valued at USD 7.66 billion in 2025 and is forecast to reach USD 20.11 billion by 2030, registering a 21.3% CAGR. Rising cyber-attacks on connected devices, stringent regulatory mandates and fast adoption of Industrie 4.0 solutions in manufacturing combine to accelerate spending on specialised security platforms. Demand concentrates on network-centric defences that safeguard operational technology, while quantum-safe cryptography investments signal long-term resilience priorities. Vendors offering hybrid cloud-edge security analytics gain traction as enterprises balance data-sovereignty rules with the need for scalable threat intelligence. Intensifying competition from niche start-ups and semiconductor players is prompting incumbents to acquire specialised capabilities, especially around AI-driven detection and secure-element design.

Europe IoT Security Market Trends and Insights

Proliferation of IoT Endpoints Enlarging Attack Surface

European enterprises added millions of sensors, gateways and robotics units during 2024, driving a 107% spike in IoT-focused attacks. Manufacturing recorded more than 500 ransomware incidents that disrupted discrete production lines and forced costly downtime. Legacy brownfield machinery integrating with IP-based networks dissolves traditional perimeters, compelling CISOs to deploy scalable zero-trust agents and secured device-management overlays. Demand for endpoint protection platforms that

remotely enforce firmware integrity and detect anomalous behaviour therefore rises across the Europe IoT Security market. Vendors that can monitor heterogeneous devices without impacting operational throughput gain competitive advantage among Industrie 4.0 adopters.

EU-wide Data-Protection Mandates Accelerating Security Spend

The NIS2 Directive, effective from October 2024, extended breach-reporting and risk-management obligations to about 350,000 European organisations. Parallel enactment of the Cyber Resilience Act compels manufacturers to embed security-by-design and maintain software bills of materials, with fines reaching EUR 15 million. Healthcare and telecom operators in France already face active audits by ANSSI following several multi-million-record breaches during 2024. Compliance urgency is translating into immediate budget reallocations toward managed detection, vulnerability management and supply-chain assessment solutions, fuelling short-term growth across the Europe IoT Security market.

Fragmented Security Standards Across Heterogeneous Devices

While ETSI EN 303 645 defines baseline controls such as removal of default passwords, differing sectoral frameworks and national certification schemes add layers of complexity. The forthcoming EU Cybersecurity Certification Scheme builds on Common Criteria but introduces new assurance classes, leaving SMEs juggling overlapping audits and spiralling consultancy fees. The SMESEC project found that 43% of attacks now target small businesses whose device portfolios span consumer and industrial categories, delaying large-scale security roll-outs.

Other drivers and restraints analyzed in the detailed report include:

Rapid Industrial-IoT Adoption in Smart Factories / Sophisticated Cyber-Attacks on Critical Infrastructure / High Integration Cost for Legacy Brown-Field Assets /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Network Security generated 38.6% revenue in 2024, underlining its foundational role in isolating industrial traffic and enforcing least-privilege segmentation. Deep-packet inspection engines tuned for Modbus, PROFINET and OPC UA mitigate lateral movement risks across converged IT-OT backbones. Inside the Europe IoT Security market size for connectivity defences, protocol-aware threat analytics are expected to grow parallel to 5G private networks that connect autonomous mobile robots on factory floors. Cloud Security, although smaller today, grows at 21.5% CAGR as enterprises shift data pipelines to hyperscale and sovereign regional clouds. Secure access service edge (SASE) offerings that converge zero-trust networking and cloud-native firewalls rank high on 2025 procurement roadmaps, positioning Cloud Security to narrow the revenue gap before 2030.

Demand for Endpoint and Application Security follows the proliferation of smart cameras, wearable sensors and micro-services that require continuous software-integrity validation. Embedded or chip-level controls such as physically unclonable functions (PUFs) appear in new automotive and healthcare devices, with semiconductor programmes co-funded under the Important Project of Common European Interest (IPCEI) fuelling uptake. Vendors delivering holistic portfolios across these layers will capture a larger slice of the Europe IoT Security market.

Software accounted for 66.5% of total spending in 2024 because enterprises prefer licence-based analytics engines that scale across hundreds of thousands of devices. Behavioural anomaly detection, secure orchestration of firmware updates and cryptographic key-lifecycle management are increasingly delivered as containerised modules easy to deploy in Kubernetes

clusters. Consequently, platform suppliers that package threat intelligence feeds and vulnerability scanners within a unified console retain high renewal rates across the Europe IoT Security market size.

Services, however, post the fastest 22.8% CAGR as SMEs lacking in-house specialists outsource threat hunting, incident response and compliance reporting. Managed security service providers (MSSPs) bundle 24□7 monitoring, penetration testing and regulatory gap assessments into subscription models attractive under tight capital budgets. Vendor-agnostic consultants that can integrate disparate security controls inside complex brownfield environments and document Cyber Resilience Act compliance are poised for sustained demand within the Europe IoT Security industry. Hardware sales remain steadier, anchored by trusted-platform modules and secure elements mandated for high-risk medical implants and automotive ECUs.

The Europe IoT Security Market Report is Segmented by Security Type (Network Security, Endpoint Security, Application Security, and More), Solution (Hardware, Software, and Services), Deployment Mode (On-Premise and Cloud), End-User Industry (Automotive and Transportation, Healthcare and Life Sciences, Government and Defence, and More), and Country. The Market Forecasts are Provided in Terms of Value (USD).

List of Companies Covered in this Report:

Cisco Systems Inc. / IBM Corporation / Thales DIS (Gemalto) / Fortinet Inc. / Infineon Technologies AG / Intel Corporation / Sophos Group PLC / Palo Alto Networks Inc. / Hewlett Packard Enterprise Co. / Broadcom Inc. (Symantec) / Trend Micro Inc. / Check Point Software Technologies Ltd. / Kaspersky Lab / ARM Ltd. / Atos SE / Siemens Digital Industries Software / Avast PLC / NXP Semiconductors N.V. / Device Authority Ltd. / Secure Thingz Ltd. /

Additional Benefits:

The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

1 INTRODUCTION
1.1 Study Assumptions and Market Definition
1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET LANDSCAPE
4.1 Market Overview
4.2 Market Drivers
4.2.1 Proliferation of IoT endpoints enlarging attack surface
4.2.2 EU-wide data-protection mandates accelerating security spend
4.2.3 Rapid industrial-IoT adoption in smart factories
4.2.4 Sophisticated cyber-attacks on critical infrastructure
4.2.5 Post-quantum-ready cryptography initiatives
4.2.6 Horizon Europe and national grants subsidising SME security upgrades
4.3 Market Restraints
4.3.1 Fragmented security standards across heterogeneous devices

4.3.2 High integration cost for legacy brown-field assets
4.3.3 Scarcity of IoT-security talent in European SMBs
4.3.4 Semiconductor supply-chain bottlenecks delaying secure-element roll-outs
4.4 Value Chain Analysis
4.5 Regulatory Landscape
4.6 Technological Outlook
4.7 Porter's Five Forces Analysis
4.7.1 Bargaining Power of Suppliers
4.7.2 Bargaining Power of Buyers
4.7.3 Threat of New Entrants
4.7.4 Threat of Substitutes
4.7.5 Intensity of Competitive Rivalry
4.8 Assessment of the Impact of Macroeconomic Trends on the Market

5 MARKET SIZE AND GROWTH FORECASTS (VALUE)
5.1 By Security Type
5.1.1 Network Security
5.1.2 Endpoint Security
5.1.3 Application Security
5.1.4 Cloud Security
5.1.5 Embedded/Chip-level Security
5.1.6 Other Niche Security Types
5.2 By Solution
5.2.1 Hardware
5.2.2 Software
5.2.3 Services
5.3 By Deployment Mode
5.3.1 On-Premise
5.3.2 Cloud
5.4 By End-User Industry
5.4.1 Automotive and Transportation
5.4.2 Healthcare and Life Sciences
5.4.3 Government and Defence
5.4.4 Manufacturing and Industrial
5.4.5 Energy and Utilities
5.4.6 Other End-User Industries
5.5 By Country
5.5.1 Germany
5.5.2 United Kingdom
5.5.3 France
5.5.4 Italy
5.5.5 Spain
5.5.6 Rest of Europe

6 COMPETITIVE LANDSCAPE
6.1 Market Concentration
6.2 Strategic Moves

6.3 Market Share Analysis
6.4 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)
6.4.1 Cisco Systems Inc.
6.4.2 IBM Corporation
6.4.3 Thales DIS (Gemalto)
6.4.4 Fortinet Inc.
6.4.5 Infineon Technologies AG
6.4.6 Intel Corporation
6.4.7 Sophos Group PLC
6.4.8 Palo Alto Networks Inc.
6.4.9 Hewlett Packard Enterprise Co.
6.4.10 Broadcom Inc. (Symantec)
6.4.11 Trend Micro Inc.
6.4.12 Check Point Software Technologies Ltd.
6.4.13 Kaspersky Lab
6.4.14 ARM Ltd.
6.4.15 Atos SE
6.4.16 Siemens Digital Industries Software
6.4.17 Avast PLC
6.4.18 NXP Semiconductors N.V.
6.4.19 Device Authority Ltd.
6.4.20 Secure Thingz Ltd.

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK
7.1 White-space and Unmet-Need Assessment

Europe IoT Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-05
		Signature	