+357 96 030922
info@marketpublishers.com

Iot Security Market Outlook 2025-2034: Market Share, and Growth Analysis By Type (Network Security, Endpoint Security, Application Security, Cloud Security, Other Types), By Component (Solution, Services), By Application

https://marketpublishers.com/r/I0EC2B8B34D7EN.html
Date: October 2025
Pages: 160
Price: US$ 3,950.00 (Single User License)
ID: I0EC2B8B34D7EN

Abstracts

The Iot Security Market is valued at USD 9.6 billion in 2025 and is projected to grow at a CAGR of 28.6% to reach USD 92.5 billion by 2034.The IoT Security Market focuses on protecting connected devices, networks, and data from cyber threats, unauthorized access, and operational disruption. As billions of devices become interconnected—across homes, factories, vehicles, and infrastructure—their attack surface increases dramatically. IoT security encompasses endpoint protection, secure communication protocols, authentication frameworks, encryption, device identity management, and threat detection. It ensures the integrity, confidentiality, and availability of IoT ecosystems, especially as these systems handle sensitive data or control critical functions. With the rise of smart cities, industrial automation, and remote healthcare, security has shifted from an afterthought to a foundational requirement. Businesses, governments, and consumers alike are prioritizing robust security strategies to safeguard their connected environments. The IoT security market saw heightened investment amid growing reports of targeted cyberattacks and botnet activity exploiting unprotected IoT endpoints. Governments introduced stricter cybersecurity regulations, such as the EU Cyber Resilience Act and the U.S. Cyber Trust Mark program, which prompted enterprises to adopt certified, secure-by-design devices. Companies like Cisco, Palo Alto Networks, and Armis launched zero-trust IoT security platforms with real-time device visibility, behavioral analytics, and automated quarantine protocols. Healthcare providers and utilities deployed anomaly detection to monitor connected devices for signs of tampering or performance deviation. Edge security became a major focus, with embedded chips and secure boot processes hardening

+357 96 030922
info@marketpublishers.com

endpoints against firmware-level attacks. Security orchestration tools also gained traction, unifying policies across cloud, edge, and legacy networks. The IoT security landscape will become more AI-driven, decentralized, and aligned with identity-centric models. Threat detection tools will use machine learning to detect and respond to subtle behavioral changes in connected devices. Blockchain-based identity systems may emerge to decentralize device authentication. As 5G and satellite IoT expand connectivity, securing devices across distributed and mobile environments will require end-to-end encryption, over-the-air updates, and real-time policy enforcement. Quantum-safe cryptography will start gaining attention, especially in defense and finance sectors. Organizations will increasingly adopt automated threat response solutions to contain breaches with minimal manual intervention. Ultimately, IoT security will evolve into a proactive, intelligent layer embedded into every phase of device and data lifecycle management.

Key Insights Iot Security Market

OG Analysis highlights the adoption of zero-trust architecture for IoT, where every device, user, and application must be verified continuously before gaining or retaining access, regardless of location or origin.

Edge device hardening is trending, with manufacturers embedding security at the hardware level—through secure boot, TPM chips, and encrypted firmware—to protect devices even before network connection.

According to OG Analysis, behavioral analytics for threat detection is growing in popularity, using AI to monitor device behavior and flag anomalies such as data spikes or command deviations in real time.

Integration of security orchestration tools is trending, allowing organizations to manage policies, detect threats, and coordinate responses across diverse cloud, edge, and on-premise IoT environments.

Regulatory compliance is increasingly shaping product development, with vendors designing devices and platforms that align with cybersecurity labeling, data privacy, and breach reporting mandates globally.

OG Analysis identifies the exponential rise in connected devices as a key driver, with more endpoints requiring visibility, authentication, and secure communication across consumer and industrial environments.

+357 96 030922
info@marketpublishers.com

High-profile cyberattacks targeting critical infrastructure and healthcare facilities are pushing organizations to implement IoT-specific security frameworks to safeguard life-critical and operational systems, says OG Analysis.

OG Analysis notes that evolving global regulations—mandating device labeling, vulnerability disclosure, and secure lifecycle practices—are accelerating investment in built-in IoT security solutions.

With growing reliance on remote operations and edge computing, businesses are prioritizing secure device provisioning, continuous monitoring, and automated threat containment to ensure service continuity.

OG Analysis highlights limited computing resources in IoT devices as a challenge, restricting the ability to implement advanced encryption, intrusion detection, and security patching on many edge endpoints.

According to OG Analysis, the lack of universal security standards and certification frameworks for IoT results in fragmented compliance approaches and inconsistent levels of protection across ecosystems.

Iot Security Market Segmentation

By Type

- Network Security
- Endpoint Security
- Application Security
- Cloud Security
- Other Types

By Component

+357 96 030922
info@marketpublishers.com

Solution

Services

By Application

Healthcare & Life Sciences

Infrastructure & Cities

Industrial System & Sensors

Smart Home & Consumer

Transport & Urban Mobility

Key Companies Analysed

Google Inc.

Microsoft Corporation

AT&T Inc.

Dell Inc.

Huawei Technologies Co. Ltd.

Hitachi DataSystems Corporation

Amazon WebServices Inc.

General Electric Company

Intel Corporation

International Business Machine Corporation

+357 96 030922
info@marketpublishers.com

CiscoSystems Inc.

Oracle Corporation

SAP SE

Fujitsu Ltd.

Hewlett-Packard Enterprise Company

Alcatel-Lucent SA

Bosch Software Innovation GmbH

Accenture plc

Autodesk Inc.

PTC Inc.

Davra Networks Limited

Cumulocity GmbH

BlackBerry Limited

C3 IoT Inc.

Exosite LLC

Device Insight GmbH

Concirrus Limited

EVRYTHNG Limited

Bright Wolf LLC

+357 96 030922
info@marketpublishers.com

Connio Inc.

Iot Security Market Analytics

The report employs rigorous tools, including Porter’s Five Forces, value chain mapping, and scenario-based modeling, to assess supply–demand dynamics. Cross-sector influences from parent, derived, and substitute markets are evaluated to identify risks and opportunities. Trade and pricing analytics provide an up-to-date view of international flows, including leading exporters, importers, and regional price trends.

Macroeconomic indicators, policy frameworks such as carbon pricing and energy security strategies, and evolving consumer behavior are considered in forecasting scenarios. Recent deal flows, partnerships, and technology innovations are incorporated to assess their impact on future market performance.

Iot Security Market Competitive Intelligence

The competitive landscape is mapped through OG Analysis’ proprietary frameworks, profiling leading companies with details on business models, product portfolios, financial performance, and strategic initiatives. Key developments such as mergers & acquisitions, technology collaborations, investment inflows, and regional expansions are analyzed for their competitive impact. The report also identifies emerging players and innovative startups contributing to market disruption.

Regional insights highlight the most promising investment destinations, regulatory landscapes, and evolving partnerships across energy and industrial corridors.

Countries Covered

North America — Iot Security market data and outlook to 2034

United States

Canada

Mexico

Europe — Iot Security market data and outlook to 2034

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

South Africa

Iran

UAE

Egypt

South and Central America — Iot Security market data and outlook to 2034

Brazil

Argentina

Chile

Peru

** We can include data and analysis of additional countries on demand.*

Research Methodology

This study combines primary inputs from industry experts across the Iot Security value chain with secondary data from associations, government publications, trade databases, and company disclosures. Proprietary modeling techniques, including data triangulation, statistical correlation, and scenario planning, are applied to deliver reliable market sizing and forecasting.

Key Questions Addressed

What is the current and forecast market size of the Iot Security industry at global, regional, and country levels?

Which types, applications, and technologies present the highest growth potential?

How are supply chains adapting to geopolitical and economic shocks?

+357 96 030922
info@marketpublishers.com

What role do policy frameworks, trade flows, and sustainability targets play in shaping demand?

Who are the leading players, and how are their strategies evolving in the face of global uncertainty?

Which regional “hotspots” and customer segments will outpace the market, and what go-to-market and partnership models best support entry and expansion?

Where are the most investable opportunities—across technology roadmaps, sustainability-linked innovation, and M&A—and what is the best segment to invest over the next 3–5 years?

Your Key Takeaways from the Iot Security Market Report

Global Iot Security market size and growth projections (CAGR), 2024-2034

Impact of Russia-Ukraine, Israel-Palestine, and Hamas conflicts on Iot Security trade, costs, and supply chains

Iot Security market size, share, and outlook across 5 regions and 27 countries, 2023-2034

Iot Security market size, CAGR, and market share of key products, applications, and end-user verticals, 2023-2034

Short- and long-term Iot Security market trends, drivers, restraints, and opportunities

Porter’s Five Forces analysis, technological developments, and Iot Security supply chain analysis

Iot Security trade analysis, Iot Security market price analysis, and Iot Security supply/demand dynamics

Profiles of 5 leading companies—overview, key strategies, financials, and products

+357 96 030922
info@marketpublishers.com

Latest Iot Security market news and developments

Additional Support

With the purchase of this report, you will receive

An updated PDF report and an MS Excel data workbook containing all market tables and figures for easy analysis.

7-day post-sale analyst support for clarifications and in-scope supplementary data, ensuring the deliverable aligns precisely with your requirements.

Complimentary report update to incorporate the latest available data and the impact of recent market developments.

** The updated report will be delivered within 3 working days*

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Iot Security Market Outlook 2025-2034: Market Share, and Growth Analysis By Type (Network Security, Endpoint Security, Application Security, Cloud Security, Other Types), By Component (Solution, Services), By Application

Product link: https://marketpublishers.com/r/I0EC2B8B34D7EN.html

Price: US$ 3,950.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/I0EC2B8B34D7EN.html