+357 96 030922
info@marketpublishers.com

IoT Security Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solution, Service), By Deployment (Cloud, On-premise), By Enterprise (SME, Large Enterprise), By Security Type (Network Security, End-point Security, Application Security, Cloud Security and Others), By Application (Smart Manufacturing, Smart Energy & Utilities, Connected Logistics, Smart Home & Consumer Electronics), By Region & Competition, 2021-2031F

https://marketpublishers.com/r/IC978BF7E1E3EN.html
Date: January 2026
Pages: 180
Price: US$ 4,500.00 (Single User License)
ID: IC978BF7E1E3EN

Abstracts

The Global IoT Security Market is projected to expand from USD 36.77 Billion in 2025 to USD 140.33 Billion by 2031, reflecting a CAGR of 25.01%. This market comprises the strategic frameworks and technological solutions necessary to protect connected devices, networks, and data against unauthorized access and cyber threats. Key drivers fueling this growth include the exponential rise in network endpoints, which broadens the global attack surface, and the enforcement of strict regulatory mandates requiring robust data protection standards. Additionally, the imperative to secure operational technology within infrastructure sectors further supports demand as organizations strive to prevent disruptions that could jeopardize safety and continuity.

Despite these drivers, the market faces a substantial challenge regarding the gap between threat awareness and actual resource allocation. The rapid adoption of complex technologies often outstrips the financial and technical commitment needed to secure them effectively. According to PSA Certified, in 2024, although 69% of

+357 96 030922
info@marketpublishers.com

technology decision-makers prioritized security more highly due to artificial intelligence, only 50% believed their organizations were investing adequate funds to address these emerging risks. This funding discrepancy highlights a financial constraint that may hinder the comprehensive implementation of advanced security measures.

Market Driver

The exponential proliferation of connected IoT devices is fundamentally widening the global attack surface, providing cybercriminals with numerous new entry points to exploit. As organizations digitize their infrastructure and consumers embrace smart technology, the sheer volume of unsecured endpoints enables threat actors to build massive botnets for distributed denial-of-service (DDoS) campaigns. This expansion of connected assets without matching security hardening has led to a dramatic increase in volumetric attacks, requiring advanced network safeguards. According to Nokia?s 'Threat Intelligence Report 2024' from March 2024, IoT botnet DDoS traffic increased fivefold over the previous year, a trend driven primarily by the exploitation of insecure devices, underscoring the critical demand for solutions that manage device visibility and neutralize botnet activity at the network edge.

Simultaneously, the market is being propelled by the escalating frequency and sophistication of malware and ransomware specifically targeting IoT endpoints. Attackers are increasingly utilizing automation to bypass traditional defenses, transforming weak IoT security into a gateway for broader enterprise network breaches. This urgency is evident in the rapid surge of malicious activity aimed at these vulnerabilities, forcing organizations to invest heavily in endpoint protection. For instance, SonicWall?s '2024 Mid-Year Cyber Threat Report' in July 2024 noted a 107% spike in IoT malware volume during the first half of the year compared to the same period in 2023. Furthermore, Check Point Software reported in 2024 that 54% of organizations on average faced attempted cyber-attacks on their IoT devices every week, further validating the need for comprehensive security measures.

Market Challenge

The Global IoT Security Market faces a significant challenge stemming from the disparity between threat awareness and actual resource allocation. While the integration of complex connected technologies is accelerating, the financial commitments required to secure these expanding ecosystems often lag behind technical necessities. This misalignment results in a precarious scenario where the sophistication of IoT networks outpaces the budgetary provisions available for their protection, effectively delaying the

+357 96 030922
info@marketpublishers.com

deployment of essential security architectures and leaving critical infrastructure vulnerable to exploitation.

This financial constraint directly impedes market expansion by limiting the wide-scale adoption of advanced defensive frameworks. According to ISACA, in 2024, 51% of organizations reported that their cybersecurity budgets were underfunded, highlighting a widespread inability to meet the rising costs of digital defense. Consequently, this funding gap compels enterprises to compromise on security depth or defer critical investments, which slows the procurement of necessary technological solutions and retards the overall revenue growth of the market despite the escalating urgency of the threat landscape.

Market Trends

The Standardization of Consumer IoT Security Labeling Programs is fundamentally reshaping the market as governments transition from voluntary guidelines to mandatory compliance regimes. This trend requires manufacturers to integrate security baselines?such as unique passwords and vulnerability disclosure policies?directly into the product lifecycle to maintain market access. Initiatives like the U.S. Cyber Trust Mark and the UK?s Product Security and Telecommunications Infrastructure (PSTI) framework are driving this shift, effectively making security certification a prerequisite for retail presence rather than a differentiator. According to a UK Government survey on the 'Cyber security of consumer IoT' from December 2024, 91% of manufacturers were aware of UK cyber security regulations related to consumer connectable products, indicating the high level of urgency surrounding these legislative requirements.

At the same time, the market is witnessing the widespread adoption of Zero Trust Architecture for IoT networks as a critical evolution beyond traditional perimeter-based defenses. Since connected devices often lack robust built-in security and operate across dispersed environments, organizations are increasingly treating every endpoint as untrusted by default, necessitating continuous verification of device identity and integrity. This architectural shift relies heavily on rigorous machine identity management, such as Public Key Infrastructure (PKI), to ensure that only authenticated assets can communicate within the network. However, the complexity of managing these identities at scale has exposed significant operational vulnerabilities; according to Keyfactor?s 'State of IoT Security' report in February 2024, 98% of organizations experienced a certificate-related outage in the past 12 months, highlighting the fragility of current systems and the pressing need for resilient zero-trust implementations.

+357 96 030922
info@marketpublishers.com

Key Market Players

Cisco Systems, Inc.

Palo Alto Networks, Inc.

Fortinet, Inc.

IBM Corporation

Check Point Software Technologies Ltd.

Trend Micro Incorporated

McAfee Corporation

Armis Security, Inc.

Forescout Technologies, Inc.

Sophos Ltd.

Report Scope

In this report, the Global IoT Security Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

IoT Security Market, By Component

Solution

Service

IoT Security Market, By Deployment

Cloud

On-premise

+357 96 030922
info@marketpublishers.com

IoT Security Market, By Enterprise

SME

Large Enterprise

IoT Security Market, By Security Type

Network Security

End-point Security

Application Security

Cloud Security and Others

IoT Security Market, By Application

Smart Manufacturing

Smart Energy & Utilities

Connected Logistics

Smart Home & Consumer Electronics

etc

IoT Security Market, By Region

North America

United States

Canada

Mexico

+357 96 030922
info@marketpublishers.com

- Europe
  - France
  - United Kingdom
  - Italy
  - Germany
  - Spain
- Asia Pacific
  - China
  - India
  - Japan
  - Australia
  - South Korea
- South America
  - Brazil
  - Argentina
  - Colombia
- Middle East & Africa
  - South Africa
  - Saudi Arabia
  - UAE

+357 96 030922
info@marketpublishers.com

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global IoT Security Market.

Available Customizations:

Global IoT Security Market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

6. NORTH AMERICA IOT SECURITY MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

7. EUROPE IOT SECURITY MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

8. ASIA PACIFIC IOT SECURITY MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

9. MIDDLE EAST & AFRICA IOT SECURITY MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

10. SOUTH AMERICA IOT SECURITY MARKET OUTLOOK

+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 - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solution, Service), By Deployment (Cloud, On-premise), By Enterprise (SME, Large Enterprise), By Security Type (Network Security, End-point Security, Application Security, Cloud Security and Others), By Application (Smart Manufacturing, Smart Energy & Utilities, Connected Logistics, Smart Home & Consumer Electronics), By Region & Competition, 2021-2031F

Product link: https://marketpublishers.com/r/IC978BF7E1E3EN.html

Price: US$ 4,500.00 (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/IC978BF7E1E3EN.html