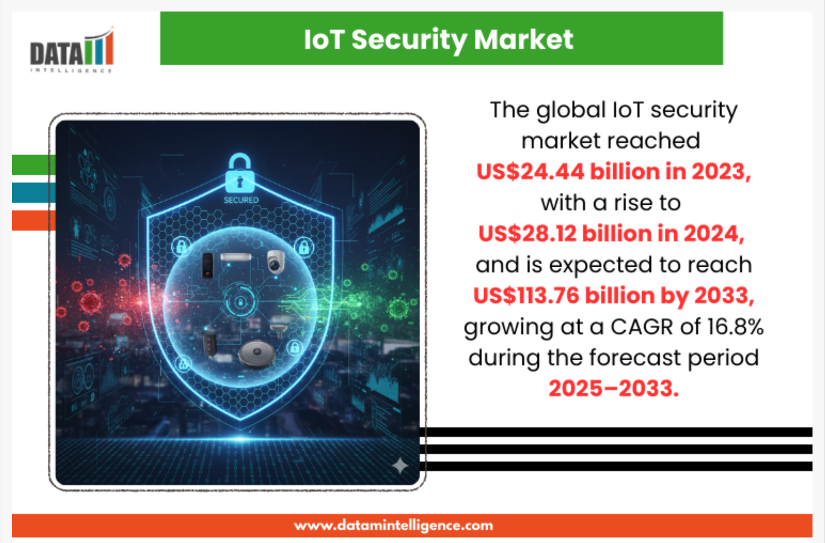
Global IoT Security Market to Surpass US$113.7 Bn by 2033, Driven by AI & Smart Device Adoption

Rising cyber threats, regulatory mandates, and explosive growth of connected devices propel the IoT security market at 16.8% CAGR.


DATAM INTELLIGENCE
IoT Security Market
SECURED
The global IoT security market reached
US$24.44 billion in 2023,
with a rise to
US$28.12 billion in 2024,
and is expected to reach
US$113.76 billion by 2033,
growing at a CAGR of 16.8% during the forecast period
2025–2033.
www.datamintelligence.com

IoT security market

AUSTIN, TX, UNITED STATES, September 29, 2025 /EINPresswire.com/ -- The global [IoT security market Size](#) is at the epicenter of digital transformation, providing the critical infrastructure and technologies needed to secure billions of connected devices across industries and applications. According to DataM Intelligence, the market stood at US$24.44 billion in 2023, rose to US$28.12 billion in 2024, and is projected to reach an impressive US$113.76 billion by 2033, registering a robust CAGR of 16.8% during 2025–2033. This phenomenal growth is fueled by the explosion of smart devices and the escalating volume of cyber-attacks targeting industrial systems, critical infrastructure, consumer electronics, and smart city initiatives worldwide.

> “With billions of devices connecting industries and cities, AI-powered IoT security is now essential for protecting critical infrastructure and ensuring regulatory compliance worldwide.”
>
> *DataM Intelligence*

□□□ □ □□□□□□ □□□□ □□□□□□□□□ □□ □□□□ □□□□□□□ (□□□□ □□□□□□□□□□ □□□□□□ □□ □□□□ □ □□□□□□ □□□□□□□□□□): https://www.datamintelligence.com/download-sample/iot-security-market

Key drivers shaping the market include the rapid deployment of IoT devices in defense, healthcare, manufacturing, and smart cities, as well as regulatory frameworks demanding improved security standards. The solutions segment leads the market due to rising demand for robust network and device protection, while North America remains the dominant geography spearheaded by government, defense, and enterprise adoption of advanced security frameworks. Meanwhile, Asia-Pacific has emerged as the fastest-growing region, underpinned by large-scale investments in smart city development and industrial digitization.

Key Highlights from the Report

 The global IoT security market is projected to reach US$113.76 billion by 2033, with a CAGR of 16.8% from 2025 to 2033.

 North America accounted for 33% of the global IoT security market share in 2024, making it the largest regional market.

 The solutions segment dominates with 65.6% market share, driven by the urgent need for cyberattack prevention and device protection.

 Asia-Pacific is the fastest-growing region, led by robust adoption in countries like Japan, China, and South Korea.

 Key growth drivers include rising cyber threats, regulatory pressures, and the proliferation of connected devices in sectors like defense, healthcare, and manufacturing.

 Major players include Microsoft, Amazon Web Services, IBM, Palo Alto Networks, Cisco Systems, and Armis Inc, all actively investing in AI-based, real-time IoT protection solutions.

Market Segmentation

The IoT security market is strategically segmented based on offering, deployment model, security type, organization size, end-user, and region to address the complex matrix of needs across diverse sectors worldwide.

By offering, the market splits into solutions and services, with the solutions segment accounting for roughly two-thirds of the overall value approximately 65.6% in 2024. Security solutions, such as comprehensive IoT threat detection, device authentication, cloud protection, and endpoint security, are seeing soaring demand as enterprises and governments contend with explosive growth in cyber risks. Vendors like Aeris have responded with integrated, agentless security platforms (e.g., Aeris IoT Watchtower) that provide real-time visibility, risk mitigation, and compliance management across vast IoT device fleets.

Deployment-wise, both cloud-based and on-premises models are prevalent. However, cloud-based solutions are steadily gaining traction due to their scalability, flexibility, and ability to facilitate faster security updates and monitoring.

By security type, the segmentation includes network security, endpoint security, application security, cloud security, and others, with network and endpoint security representing the backbone of most organizational IoT security approaches.

Organization size also plays a crucial role, as large enterprises account for the bulk of investments in advanced IoT security while small and medium-sized businesses (SMBs) often face resource constraints that hinder widespread adoption. End-user segmentation encompasses industries such as healthcare, automotive, manufacturing, energy & utilities, and consumer electronics, among others each sector having unique security needs, regulatory requirements, and complexities.

Regional Insights

The North America region leads the global IoT security market, accounting for 33% of the market in 2024. This dominance reflects strong government, defense, and enterprise investment in cyber protection, advanced R&D capacity, as well as robust collaborations between commercial vendors and federal agencies. For example, high-profile threats such as PRC-linked botnets have pressed agencies including the NSA, FBI, and US Cyber Command to adopt comprehensive IoT security programs. The region is also a testing ground for evolving cybersecurity labeling initiatives intended to spur greater IoT protection.

Asia-Pacific is the fastest-growing geography, driven by aggressive smart city rollouts (notably in Japan’s “Society 5.0” and China’s extensive urban digitization), industrial modernization, and progressive frameworks like Japan’s JC-STAR IoT Product Security Labeling Scheme. Regional governments and industries have quickly adopted AI-powered threat monitoring and fostered global partnerships to strengthen IoT infrastructure protection and ensure resilience in mission-critical public and private applications.

Europe also plays a substantial role, particularly as key economies bolster their regulatory frameworks, promote public-private partnerships, and invest in the cybersecurity of healthcare, energy, and industrial assets. Meanwhile, other regions including South America and Middle East & Africa are witnessing market expansion, albeit at a more gradual pace, as awareness and investments gradually increase in response to rising threats and regulatory initiatives.

Market Dynamics

Market Drivers

The IoT security market is propelled by the escalating prevalence of cyber threats—ransomware, AI-powered attacks, and vulnerabilities exploitations—targeting billions of connected assets in enterprise, industrial, and consumer environments. Organizations urgently seek AI-driven, real-time detection and incident response solutions that can preempt, neutralize, and mitigate potential breaches at the device, edge, and network layer. Regulatory mandates and growing cyber risk awareness further drive adoption, with organizations investing in holistic platforms capable of enforcing compliance, threat intelligence, and proactive response.

Market Restraints

Despite robust need, high costs of deployment and ongoing management present a considerable adoption barrier, especially for smaller organizations. Cutting-edge security solutions demand significant upfront investments for hardware/software integration, skilled personnel, and ongoing compliance. SMBs are particularly challenged by these costs, often restricting adoption to more modest, less comprehensive options—leaving critical vulnerabilities exposed. Additionally, the rapidly evolving threat landscape means organizations must continually invest in monitoring, updates, and AI models to maintain robust defense, straining budgets.

Market Opportunities

Opportunities abound in the development of cost-effective, scalable security architectures tailored for resource-constrained SMBs and vertical-specific environments. Innovations such as AI/ML-powered analytics, agentless monitoring, cloud-native protection, and compliance automation create possibilities for broader adoption and market expansion. The explosion of smart cities, healthcare IoT, autonomous vehicles, and industrial automation opens new frontiers for specialized solutions that fuse physical and cyber security disciplines. Additionally, as regulatory standards tighten globally, vendors can differentiate on compliance expertise and turnkey integration capabilities, fueling growth.

Get Customization in the report as per your requirements:
https://www.datamintelligence.com/customize/iot-security-market

Reasons to Buy the Report

- Gain comprehensive insights on market size, share, and CAGR projections with accurate, up-to-date statistics from DataM Intelligence.
- Understand key trends, growth drivers, restraints, and emerging opportunities shaping the IoT security landscape.
- Benchmark competitive dynamics—analyze market leaders, their offerings, and newest technological advancements.
- Evaluate regional trends to optimize go-to-market strategies and investments by geography.
- Access robust segmentation analysis, providing actionable intelligence across product types, end-users, and security types.

Frequently Asked Questions (FAQs)

- How big is the global IoT security market?
- Who are the key players in the global IoT security market?
- What is the projected CAGR of the IoT security market for 2025–2033?
- Which region is forecast to dominate the IoT security industry?
- What opportunities exist for innovative IoT security vendors?

Company Insights

- Microsoft
- Amazon Web Services, Inc.
- Google
- IBM
- Cisco Systems, Inc.
- Fortinet, Inc.
- Palo Alto Networks, Inc.
- Armis Inc
- Thales
- Allot

Recent Developments:

- In September 2025, Cisco launched an AI-powered IoT security platform for enterprise and industrial networks. The system monitors device behavior in real-time to detect anomalies. Early adoption shows improved threat detection and reduced network breaches.

- In August 2025, Palo Alto Networks expanded its IoT security suite with automated threat intelligence and device profiling. The platform protects critical infrastructure and smart manufacturing systems. Initial deployments highlight faster response to vulnerabilities and enhanced network resilience.

Conclusion

The global IoT security market is on a steep growth trajectory as organizations worldwide recognize the critical need to secure their expanding networks of connected devices. With DataM Intelligence projecting market value to exceed US$113 billion by 2033, the sector is set for remarkable transformation, driven by regulatory momentum, technological innovation, and heightened demand for comprehensive, AI-powered security solutions. As advanced threats accelerate and industries from defense to healthcare deepen their reliance on IoT, market leaders and innovators stand poised to redefine the future of secure, connected enterprise and smart city ecosystems.

Sai Kiran
DataM Intelligence 4market Research LLP
877-441-4866
sai.k@datamintelligence.com
Visit us on social media:
LinkedIn
X

This press release can be viewed online at: https://www.einpresswire.com/article/853464198