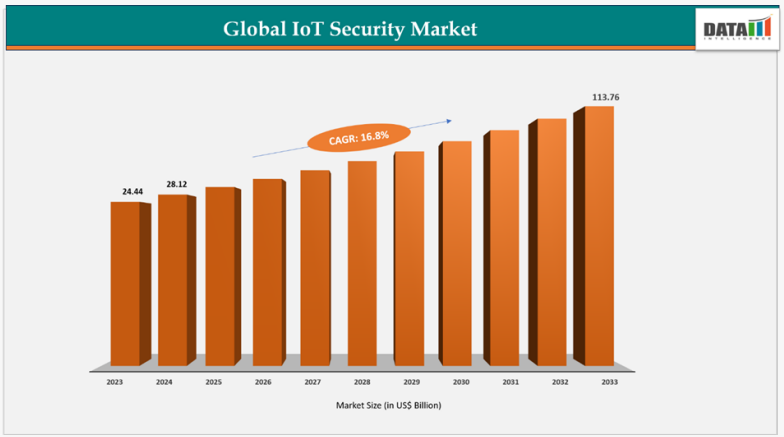
IoT Security Market Accelerates as Cyber Threats Rise Across Connected Ecosystems

Rapid IoT adoption in industry, healthcare, and smart cities fuels demand for advanced security solutions, driving the market toward US$ 113.8 billion by 2033.



IoT Security

AUSTIN, TX, UNITED STATES, December 18, 2025 /EINPresswire.com/ -- According to DataM Intelligence, the global IoT security market reached US$ 24.44 billion in 2023 and increased to US$ 28.12 billion in 2024, with projections indicating it will grow significantly to US$ 113.76 billion by 2033, expanding at a strong CAGR of 16.8% during the forecast period 2025–2033. Market growth is being driven by the rapid proliferation of connected devices across defense, smart cities, healthcare, manufacturing, and critical infrastructure, alongside a sharp rise in cyber threats targeting IoT ecosystems. Organizations are increasingly adopting AI-driven threat detection, secure device authentication, endpoint protection, and network security solutions, supported by strategic partnerships, regulatory initiatives, and growing awareness of IoT-related vulnerabilities.

> As connectivity expands, security becomes the foundation of trust. Robust, AI-driven IoT security is essential to safeguard data, infrastructure, and the future of digital ecosystems."
>
> *DataM Intelligence*

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

Regionally, the United States dominates the IoT security market, supported by robust defense spending, enterprise digitalization, and critical infrastructure protection needs. Government initiatives, including the development of a cybersecurity labeling program for IoT devices, along with strong R&D capabilities and collaboration between technology providers and security vendors, continue to reinforce market leadership. Meanwhile, Japan is emerging as a key growth market, driven by ambitious smart city programs such as Society 5.0 and advanced urban

mobility projects. The increasing reliance on connected urban systems is making cybersecurity a top priority, accelerating adoption of AI-based monitoring and global technology partnerships to ensure secure and resilient IoT deployments.

IoT Security

Key Highlights from the Report
 The IoT security market is witnessing rapid growth due to the explosion of connected devices worldwide.

 Network security and device management solutions account for a significant share of market revenue.

 Industrial IoT (IIoT) security is a major growth driver due to rising cyber risks in critical infrastructure.

 North America leads the global market, driven by high cybersecurity investments and regulatory compliance.

 Cloud-based IoT security solutions are gaining strong traction among enterprises.

 Increasing regulatory pressure is accelerating adoption of end-to-end IoT security frameworks.

Market Segmentation
The IoT security market segmentation reflects the complexity of IoT ecosystems and the diverse security needs across industries and deployment environments.

- By solution type, the market includes network security, endpoint security, application security, cloud security, and data security solutions. Network security dominates the segment as IoT devices rely heavily on continuous connectivity, making networks a prime target for cyberattacks. Endpoint security is gaining momentum as organizations seek to secure devices at the hardware and firmware level, preventing unauthorized access and malware infiltration.

- By service, the market comprises professional services and managed security services. Professional services include consulting, integration, and deployment, helping organizations design tailored IoT security architectures. Managed security services are witnessing strong growth as enterprises outsource monitoring, threat detection, and incident response to

specialized providers due to skill shortages and increasing complexity of IoT environments.

- By deployment mode, IoT security solutions are categorized into on-premises and cloud-based deployments. On-premises solutions remain prevalent in highly regulated industries such as defense, energy, and healthcare, where data sovereignty and control are critical. However, cloud-based IoT security is growing at a faster pace due to scalability, cost efficiency, and seamless integration with cloud-native IoT platforms.

- By end-user industry, the market serves manufacturing, healthcare, energy & utilities, transportation & logistics, smart cities, consumer electronics, and defense & government. Manufacturing and industrial IoT represent the largest end-user segment, as cyberattacks on operational technology (OT) systems can lead to severe financial losses, safety risks, and production downtime. Healthcare IoT security is also expanding rapidly due to increased adoption of connected medical devices and remote patient monitoring systems.

Regional Insights
- North America holds the largest share of the global IoT security market, driven by widespread IoT adoption, advanced digital infrastructure, and stringent cybersecurity regulations. The United States leads the region, supported by strong investments in smart manufacturing, healthcare IoT, and critical infrastructure protection. The presence of leading cybersecurity vendors and technology innovators further strengthens regional market growth.

- Europe represents a significant market, supported by strict data protection regulations such as GDPR and increasing focus on securing smart cities and industrial automation systems. Countries including Germany, the UK, and France are actively investing in IoT security to protect critical infrastructure, energy grids, and connected transportation systems.

- The Asia-Pacific region is expected to witness the fastest growth during the forecast period. Rapid industrialization, large-scale smart city projects, and expanding consumer IoT adoption in countries such as China, India, Japan, and South Korea are driving demand for IoT security solutions. Governments in the region are also introducing cybersecurity frameworks to address growing digital risks.

- Latin America, the Middle East, and Africa are emerging markets for IoT security, driven by increasing digitalization of utilities, oil & gas, and transportation sectors. While adoption remains at an early stage, rising awareness of cyber threats and growing IoT investments are expected to fuel steady growth.

Market Dynamics
1) Market Drivers

The primary driver of the IoT security market is the rapid proliferation of connected devices across industrial, commercial, and consumer applications. As IoT ecosystems grow in scale and complexity, so does the risk of cyberattacks, data breaches, and system disruptions. High-profile incidents involving compromised smart devices and critical infrastructure have heightened awareness and accelerated investments in IoT security. Additionally, stringent regulatory and compliance requirements related to data privacy and critical infrastructure protection are compelling organizations to implement robust security measures.

2) Market Restraints
Despite strong growth prospects, the market faces challenges such as lack of standardization and interoperability across IoT platforms and devices. Many IoT systems are built using proprietary technologies, making it difficult to implement uniform security frameworks. Furthermore, budget constraints and limited cybersecurity expertise, particularly among small and medium-sized enterprises, can hinder adoption of comprehensive IoT security solutions.

3) Market Opportunities
The IoT security market presents substantial opportunities through the integration of artificial intelligence, machine learning, and behavioral analytics for advanced threat detection and prevention. The expansion of 5G networks is enabling new IoT use cases, creating demand for next-generation security solutions capable of handling high-speed, low-latency environments. Additionally, growing adoption of zero-trust security models and hardware-based security is expected to unlock new growth avenues over the forecast period.

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

Reasons to Buy the Report
 Gain detailed insights into the global IoT security market size, trends, and growth forecasts.
 Understand emerging threats and security technologies shaping IoT ecosystems.
 Identify high-growth industries and regions for strategic investment decisions.
 Analyze competitive strategies and innovation trends among leading IoT security providers.
 Support informed planning with reliable data and expert analysis from DataM Intelligence.

Frequently Asked Questions (FAQs)
 How big is the global IoT security market today?
 Who are the key players in the global IoT security market?
 What is the projected growth rate of the IoT security market?
 What is the market forecast for IoT security by 2033?
 Which region is estimated to dominate the IoT security industry during the forecast period?

Company Insights
Key players operating in the IoT security market include:
• Cisco Systems, Inc.

• IBM Corporation
• Microsoft Corporation
• Palo Alto Networks
• Fortinet, Inc.
• Check Point Software Technologies
• Broadcom Inc.
• Thales Group

Recent Developments
- In November 2025, Cisco Systems expanded its IoT security portfolio with advanced zero-trust network access capabilities designed to protect large-scale industrial IoT deployments, supported by increased R&D investment.

- In October 2025, Microsoft enhanced its cloud-based IoT security platform by integrating AI-driven threat detection and automated response features, strengthening security for enterprise and smart city IoT environments.

Conclusion
The IoT security market is entering a phase of accelerated growth as connected devices become deeply embedded in critical business operations and everyday life. As highlighted by DataM Intelligence, the market's strong growth trajectory through 2033 is underpinned by rising cyber threats, regulatory pressure, and continuous innovation in security technologies. Organizations that prioritize end-to-end IoT security spanning devices, networks, applications, and data will be better positioned to mitigate risks and unlock the full potential of IoT-driven digital transformation. With ongoing advancements in AI, cloud computing, and zero-trust architectures, IoT security will remain a vital enabler of secure, resilient, and scalable connected ecosystems worldwide.

Related Reports:
1) Industrial Cybersecurity Market

2)Embedded Security Market

Sai Kiran
DataM Intelligence 4market Research LLP
+ +1 877-441-4866
sai.k@datamintelligence.com
Visit us on social media:
LinkedIn
YouTube
X