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

Market Report | 2025-04-28 | 100 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:

The North America IoT Security Market size is estimated at USD 11.94 billion in 2025, and is expected to reach USD 32.23 billion by 2030, at a CAGR of 21.97% during the forecast period (2025-2030).

Key Highlights
- The emerging business models and applications, coupled with the reducing device costs, have been instrumental in driving the adoption of IoT, consequently, the number of connected devices, such as connected machines, wearables, cars, meters, and consumer electronics.
- Attacks on consumer IoT devices are prevalent, and the overall possibility of disruption in manufacturing and similar industries makes the threat more serious. Various end-user industries in the United States and Canada have faced considerable security attacks in various industries in the past few years. IoT security is becoming a significant focus area for businesses, consumers, and regulators. Following such increasing prominence, enterprises that are offering IoT-based solutions worldwide are investing heavily in the security aspect of these solutions.
- For instance, in October 2022, Datadog, Inc., the monitoring and security platform for cloud applications, declared the general availability of Cloud Security Management. This product brings together capabilities from Cloud Security Posture Management (CSPM), Cloud Workload Security (CWS), alerting, incident management, and reporting in a single platform to enable DevOps and Security teams to identify misconfigurations, detect threats, and secure cloud-native applications.
- Moreover, the increasing dependency on connected devices is creating the need to keep the connected devices secure. This significant growth is anticipated to be driven by the growing industry focus on deploying a connected ecosystem as well as the standardization of 3GPP cellular IoT technologies.
- With the growing number of devices connected to the Internet, the cyber world is anticipated to witness a significant rise in the occurrence and emergence of new threats and attacks. IoT devices are particularly vulnerable to various network attacks, such as

data theft, spoofing, phishing attacks, and DDoS attacks (denial of service attacks). These can lead to various cybersecurity-related threats like ransomware attacks and other serious data breaches that can take businesses a lot of money and effort to recover from.
- However, the growing complexity among devices, coupled with the lack of ubiquitous legislation, could be a major matter of concern that can limit the overall market's growth throughout the forecast period.
- Since the beginning of COVID-19, there has been an increase in IoT attacks, and hence, countries worldwide have implemented several preventive measures. With communities being asked to stay at home and schools being closed, multiple organizations have found a way to allow their employees to work from their homes. This has resulted in a rise in the adoption of video communication platforms. Moreover, during the post-COVID-19 period, the market is expected to witness significant growth opportunities, especially due to the introduction of various cost-effective cloud-based and hybrid solutions by the leading major market participants.

North America IoT Security Market Trends

Increasing Number of Data Breaches is Anticipated to Drive the Market

- With the increase in the number of devices connected to the Internet, the cyber world is expected to witness a rise in the occurrence and emergence of new threats and attacks. This is evident by the growth in data breaches across the North America region in various end-user verticals over the past few years. These attacks, which directly target business systems and individuals, may potentially lead to enormous financial and personal losses. Thus fueling the need for IoT security for consumer devices that are highly susceptible to data breaches.
- Moreover, the growth in data breaches across the region in various end-user industries, such as healthcare, manufacturing, BFSI, automotive, etc., is driving the need for IoT security solutions to protect their connected devices from cyberattacks. For instance, according to the ITRC 2022 Annual Data Breach Report by Identity Theft Resource Center, the number of data compromises in the United States was 1802 cases in 2022. The number of data compromises in the United States significantly increased from 157 cases in 2005 to 1802 cases in 2022.
- Further, cloud services are experiencing high adoption rates owing to the demand for IoT. This increasing use of cloud systems across various verticals has increased the vulnerabilities of these systems to data breaches. With many providers offering multiple solutions, the need for a uniform security platform is rising. IoT security can be deployed for devices and communication, data storage, and lifecycle solutions.
- Additionally, the market is further expected to grow due to the increasing government initiatives to protect businesses from cyberattacks. For instance, in July 2023, The Biden administration launched an Internet of Things (IoT) cybersecurity labeling program to protect Americans against the myriad security risks associated with internet-connected devices. The program, "U.S. Cyber Trust Mark," aims to help Americans ensure they are buying internet-connected devices that include strong cybersecurity protections against cyberattacks.

United States is Expected to Dominate the Market

- The major crucial factors for the growth of the IoT security market in the United States are the high adoption of advanced technologies, increasing cyberattacks, and a growing number of connected devices in the country. The country is one of the dominant regions for IoT deployment. Other factors include the growth in digitalization and IoT security spending in the region.
- Moreover, the region houses significant IoT Security vendors, including Symantec Corporation, IBM Corporation, FireEye Inc., and Palo Alto Networks Inc., among others. The vendors are strengthening their product portfolio and market presence by

boosting their product innovation. For instance, in March 2022, Palo Alto Networks, a provider of network firewalls, declared that it has teamed up with Amazon Web Services to unveil the new Palo Alto Networks Cloud NGFW for AWS, a managed Next-Generation Firewall (NGFW) service designed to simplify securing AWS deployments, allowing organizations to speed their pace of innovation while remaining highly secure.
- Also, in May 2022, STMicroelectronics, a global semiconductor provider serving customers across the spectrum of electronics applications, revealed the details of its collaboration with Microsoft, an ST-authorized partner. The aim was to strengthen the security of emerging Internet-of-things applications. ST is combining its ultra-low-power STM32U5 microcontrollers with Microsoft Azure RTOS & IoT Middleware as well as a certified secure implementation of the Arm Trusted Firmware -M (TF-M) secure services, especially for embedded systems.
- Moreover, the United States is experiencing an increasing number of cyber threats. According to the Identity Theft Resource Center, the average number of breaches in the country has increased marginally over the past few years. In October 2022, The Biden-Harris Administration brought a significant focus to improving the United States' cyber defenses, building a comprehensive approach to take aggressive action to strengthen and safeguard the nation's cybersecurity.
- As per GSMA Intelligence, the total number of industrial and consumer Internet of Things connections in North America is forecast to grow to around 5.4 billion by the end of the year 2025. In 2019, the total number of IoT connections in North America amounted to 2.8 billion connections. Such a significant rise in the overall count of the industrial and consumer Internet of Things connections within the region is expected to propel the market's overall growth opportunities significantly.

North America IoT Security Industry Overview

The competitive landscape of the North American IoT Security Market is characterized by fragmentation due to the presence of numerous regional players across the region. These market participants are increasingly introducing innovative solutions to cater to various industries. Furthermore, the market is experiencing a notable increase in collaborations and acquisitions aimed at enhancing its market presence.

In December 2022, Check Point Software Technologies Ltd., a cybersecurity solutions provider, unveiled Check Point Quantum Titan, an enhancement to the Check Point Quantum cyber security platform. The Quantum Titan release incorporates three software blades that harness the power of deep learning and artificial intelligence (AI) to offer advanced threat prevention against sophisticated domain name system exploits (DNS) and phishing attacks, as well as autonomous IoT security. With Check Point Quantum Titan, the platform now includes IoT device discovery and the automatic application of zero-trust threat prevention profiles to safeguard IoT devices.

In December 2022, Palo Alto Networks introduced Medical IoT Security, a comprehensive Zero Trust security solution designed for medical devices. This solution enables healthcare organizations to securely and rapidly deploy and manage new connected technologies. The zero-trust approach to cybersecurity focuses on continuously verifying every user and device, thereby eliminating implicit trust within the organization's security framework.

Additional Benefits:

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

Table of Contents:

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

Market Report | 2025-04-28 | 100 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	2026-02-28
		Signature