

Report Information

More information from: <https://www.marketresearchfuture.com/reports/healthcare-iot-security-market-946>

Healthcare IoT Security Market Research Report - Forecast till 2030

Report / Search Code: MRFR/HCIT/0440-CR

Publish Date: August, 2019

[Request Sample](#)

Price	1-user PDF : \$ 4950.0	Enterprise PDF : \$ 7250.0
-------	------------------------	----------------------------

Description:

Healthcare IoT security Market Overview: Healthcare IoT Security Market is expected to reach USD 1.12 billion by 2030 at 18.80% CAGR during the forecast period 2022-2030. In traditional times patients used to book appointments with doctors for their check-ups and routine calls or used to use the medium of phones to connect with doctors limiting the point of contact and communication. But, with the introduction of the internet of things, patients and doctors were connected using the internet in the healthcare department. Now doctors can monitor their patients remotely using cameras, microphones, teleprompters, etc. Artificial intelligence with machine learning developed programs and algorithms for healthcare departments for countries to track and record patient-doctor data which can be used globally concerning patient's consent. With increased global access to IoT in healthcare (Internet of Things), security solutions were introduced to maintain the security and decorum of the medical industry.

With modernization, technology has boosted to a greater level which has led the hospitals to come to homes for tracking and maintaining patients. The introduction of insulin pumps, pacemakers, heartbeat monitors, nasal pumps, and other devices like smartphones and watches to monitor human health has made for the healthcare IoT security market. Government and private organizations play a vital role in maintaining the security of all the home hand-held devices and healthcare institutions.

COVID-19 Analysis:

In the November of 2019, the world woke up to an outbreak of a worldwide pandemic that affected countries economically and politically. With the immense loss of man-power countries, economical wealth came to a stand-still. Many countries like Russia, Italy, Brazil, etc. population was diminished to a considerable amount and other countries like the US, India, UK, etc. are facing a rise in active COVID-19 cases on daily basis. Global lockdowns were imposed countrywide and further state-wise to contain the spread of the virus. The Healthcare industry in coordination with the government has played a vital role in tracking and recording the patients and treating them. Healthcare IoT Security Market has shown a boost due to an increased state of emergency to isolate the patients depending on their symptoms and treating them accordingly. Sharing patient's data is at risk and can hamper patient's credibility thus highly secure systems were imposed to share the information across the network.

Healthcare IoT security Market Dynamics:

Drivers:

Healthcare IoT Security Market is on the verge of growing globally due to the increased demand for real-time data processing of patient records. More customers are inclined in booking doctor's appointments online using hospital services that maintain a schedule between doctor and customer. This helps in the time saving of both customers and doctors by helping in removing the waiting queue. The government of all the 213 countries in the world is concerned with patient-doctor confidentiality thus has imposed HIPPA training for hospital employees to adhere to security. Nowadays our smartphones and watches are acting as health tracking data like a heartbeat monitor, blood pressure, insulin levels, oxygen levels, glucose levels, etc. which needs to be secured to avoid cybercrimes.

Challenges:

The major threats that involve the healthcare IoT security industry are easy passwords, poor authentication, loss of data while transfer due to poor network, and other cybercrimes. With an increase in the world's population, there is an increase in patient inventory thus storing the data on-premise has become tougher with time. Thus, cloud-based storage came into the picture. On one hand, this led to easy data access and communication between doctors and patients, but on the other hand, cyber hacking and attacks on internet-connected devices became more vulnerable due to non-secure networks and failed firewall protections.

Technology Analysis:

Conventional storage systems are no prompted in healthcare systems due to the introduction of artificial intelligence (to predict the early onset of diseases by analyzing the patient's recording using deep learning). Thus, IoT (Internet of Things) was introduced in the healthcare department where patient's illness history, bill payments, mode of payment, name, age, date of visit, etc. were recorded and stored in hospitals inventory. This in turn is shared across platforms using network hubs making a well connected healthcare system. To maintain cybersecurity government has imposed rules and regulations that each healthcare institution must follow while implementing IoT in the regions to maintain customer satisfaction and security.

Segment Overview:

By Type:

Healthcare IoT Security Market is segmented as identity management, data loss prevention, access management, data encryption, threat management, system virus management, and data analysis. When a hospital or healthcare center implements IoT Security measures it must follow protocols to maintain security against threats and cybercrimes. A secured ERP system is made for entering the customer's data with is stored in XML files secured by passwords. Virus protection software is installed to fight against unnecessary threats of computer and internet viruses while uploading and downloading documents. Firewalls are initiated to provide prevention against hacking of hardware devices associated with patient monitoring.

By Vertical:

Healthcare IoT Security Market is segmented majorly into three categories based on vertical namely: biotechnology (used to maintain the security of user data), Pharma security (used to maintain the security of pharma department against unnecessary threats towards the drug testing or discovery of new drugs or sabotaging the contents of already authorized drugs) and medical device security (used to avoid the hacking of hardware devices associated with patient monitoring).

Regional Analysis:

Healthcare IoT security market trends show development in the private and public healthcare sector where authorities are more concerned with maintaining the industrial standards with agreeing to government regulations. North America is the top-most player when it comes to Healthcare IoT security by securing a global market share of more than 40% in regional accounting and adapting healthcare services to IoT security and privacy. Europe (Russia, Germany, etc.) has contributed about 20% to the global healthcare security market by adhering to global security standards. Asia-Pacific (China, Japan, India, Singapore) have contributed about 40% to new clinical trials of chronic diseases as read by WHO contributing to the rapid increase of the healthcare IoT security industry. Independently Asia-Pacific regions have contributed a CAGR of 47% to the healthcare industry rising the market quotient and revenue by about 2.8 million dollars in the past decade.

Competitive Landscape:

The Healthcare IoT security industry has shown tremendous growth since the late 2000s due to increased internet usage throughout the world making it a daily need. The Healthcare IoT security Market has seen a greater number of rural and urban healthcare centers invest in IoT security trends. Many companies have invested in security and firewall-providing industries giving rise to competition between them to prove their worth. Microsoft (US), IBM, Oracle, Intel, Cisco Systems, Deutsche Telekom AG, Agile Cyber Security, Checkpoint Software Technology, Fortinet Inc, Inside Secure SA, Eurotech, Kaspersky, etc., are few of the market key players of healthcare IoT security systems. With more digitalization and artificial intelligence to draw a productive analysis of patient's and doctor's data and chronic diseases, it has become essential to secure healthcare data against any sort of cyber and physical crime that hampers customer's credibility.

Recent Developments:

Cisco Systems is one of the best securities providing companies in terms of secured VPNs and two-factor authentication that ensures secure login. Many companies like Oracle, IBM, etc. have been using CISCO security to authenticate the server access to various healthcare industry's data like Pfizer, Ranbaxy. Recently it also acquired a stake of about 1.3 Billion US dollars in Jasper technology to provide a secure connection to maintain healthcare data. Kaspersky and WiSekey have been working in collaboration since 2016 to maintain end-to-end security between network hubs for secure and authenticated data transfer. Oracle has used strict firewalls to connect with outside servers to maintain healthcare data entries of companies.

Report Overview:

Healthcare IoT Security Market involves end-to-end data security on the cloud-based storage involving the application and network security. Most of the pharmaceutical industries and medical centers have adapted to Healthcare IoT Security companies to maintain the decorum of customer's data. With an increased demand for security for patient's data and real-time data, America, Europe, China, India, Japan, Australia have invested in Healthcare IoT Security Market trends leading to more use of AI and deep learning to process and store this information for maintaining security.

Table of Content:

Contents
1 EXECUTIVE SUMMARY
2 MARKET INTRODUCTION
2.1. Definition
2.2. Assumptions & Limitations
3 RESEARCH METHODOLOGY
3.1. Research Process
3.2. Primary Research
3.3. Secondary Research
3.4. Market Size Estimation
4 MARKET DYNAMICS
4.1. Overview
4.2. Drivers
4.2.1. Increased Data Privacy Concerns Among Consumers
4.2.2. Increased Government Concerns Over Healthcare IoT Security
4.2.3. Increased Usage Of Smart Devices For Health Management
4.2.4. Increased Proliferation Of Cyber Crimes In Healthcare
4.3. Restraints
4.4. Opportunities
5 MARKET FACTOR ANALYSIS

- 5.1. Value Chain Analysis
 - 5.1.1. R&D And Designing
 - 5.1.2. Manufacturing
 - 5.1.3. Distribution & Sales
 - 5.1.4. Post-Sales Review
- 5.2. Porter's Five Forces Model
 - 5.2.1. Bargaining Power Of Suppliers
 - 5.2.2. Bargaining Power Of Buyers
 - 5.2.3. Threat Of New Entrants
 - 5.2.4. Threat Of Substitutes
 - 5.2.5. Intensity Of Rivalry
- 5.3. Recent FDA Approvals
- 6 GLOBAL BARIATRIC SURGERY DEVICES MARKET, BY COMPONENT
 - 6.1. Introduction
 - 6.2. Surgical Stapler
 - 6.2.1. Analytics
 - 6.2.2. Encryption
 - 6.2.3. Data Loss Protection
 - 6.2.4. Identity And Access Management
 - 6.2.5. Unified Threat Management
 - 6.2.6. Others
 - 6.3. Services
 - 6.3.1. Consulting Services
 - 6.3.2. Risk Assessment Services
 - 6.3.3. Design & Integration Services
 - 6.3.4. Managed Security Services
 - 6.3.5. Others
- 7 GLOBAL BARIATRIC SURGERY DEVICES MARKET, BY SECURITY TYPE
 - 7.1. Introduction
 - 7.2. Application Security
 - 7.3. Cloud Security
 - 7.4. Endpoint Security
 - 7.5. Network Security
 - 7.6. Others Security
- 8 GLOBAL BARIATRIC SURGERY DEVICES MARKET, BY APPLICATION
 - 8.1. Introduction
 - 8.2. Pharmaceutical
 - 8.3. Medical Devices
 - 8.4. Biotechnology
 - 8.5. Others
- 9 GLOBAL BARIATRIC SURGERY DEVICES MARKET, BY REGION
 - 9.1. Overview
 - 9.2. Americas
 - 9.2.1. North America
 - 9.2.1.1. US
 - 9.2.1.2. Canada
 - 9.2.2. Latin America
 - 9.3. Europe
 - 9.3.1. Western Europe
 - 9.3.1.1. Germany
 - 9.3.1.2. France
 - 9.3.1.3. UK
 - 9.3.1.4. Italy
 - 9.3.1.5. Spain
 - 9.3.1.6. Rest Of Western Europe
 - 9.3.2. Eastern Europe
 - 9.4. Asia-Pacific
 - 9.4.1. China
 - 9.4.2. India
 - 9.4.3. Japan
 - 9.4.4. South Korea
 - 9.4.5. Australia
 - 9.4.6. Rest Of Asia-Pacific
 - 9.5. Middle East & Africa
 - 9.5.1. Middle East
 - 9.5.2. Africa
- 10 COMPETITIVE LANDSCAPE
 - 10.1. Overview
 - 10.2. Competitive Analysis
- 11 COMPANY PROFILE
 - 11.1. Inside Secure SA
 - 11.1.1. Company Overview
 - 11.1.2. Financial Overview
 - 11.1.3. Products Offering
 - 11.1.4. Key Developments
 - 11.1.5. SWOT Analysis
 - 11.1.6. Key Strategy
 - 11.2. IBM Corporation
 - 11.3. Cisco Systems Inc.
 - 11.4. Intel Corporation
 - 11.5. Oracle Corporation
 - 11.6. Sophos Group Plc
 - 11.7. Symantec Corporation
 - 11.8. Trend Micro Inc.
 - 11.9. Checkpoint Software Technology
 - 11.10. Kaspersky Labs
 - 11.11. Fortinet Inc
 - 11.12. Intelen Inc.
 - 11.13. Eurotech SpA
 - 11.14. Deutsche Telekom AG
 - 11.15. SecureFLO LLC
 - 11.16. Dell Corporation
 - 11.17. Atmel Corporation

11.18. Security Mentor
11.19. Klynveld Peat Marwick Goerdeler
11.20. Agile Cyber Security Solutions, LLC
11.21. Others
12 APPENDIX
12.1. References
12.2. Related Reports
13 List Of Tables
Table 1 Global Healthcare IoT Security Market Synopsis, 2020–2027
Table 2 Global Healthcare IoT Security Market Estimates And Forecast, 2020–2027 (USD Million)
Table 3 Global Healthcare IoT Security Market, By Region, 2020–2027 (USD Million)
Table 4 Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 5 Global Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 6 Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 7 North America: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 8 North America: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 9 North America: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 10 US: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 11 US: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 12 US: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 13 Canada: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 14 Canada: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 15 Canada: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 16 Latin America: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 17 Latin America: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 18 Latin America: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 19 Europe: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 20 Europe: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 21 Europe: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 22 US: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 23 Western Europe: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 24 Western Europe: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 25 Eastern Europe: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 26 Eastern Europe: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 27 Eastern Europe: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 28 Asia-Pacific: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 29 Asia-Pacific: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 30 Asia-Pacific: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
Table 31 Middle East & Africa: Global Healthcare IoT Security Market, By Component, 2020–2027 (USD Million)
Table 32 Middle East & Africa: Healthcare IoT Security Market, By Security Type, 2020–2027 (USD Million)
Table 33 Middle East & Africa: Global Healthcare IoT Security Market, By Application, 2020–2027 (USD Million)
14 List Of Figures
Figure 1 Research Process
Figure 2 Segmentation For Global Healthcare IoT Security Market
Figure 3 Segmentation Market Dynamics For Global Healthcare IoT Security Market
Figure 4 Global Healthcare IoT Security Market Share, By Component, 2020
Figure 5 Global Healthcare IoT Security Market Share, By Security Type, 2020
Figure 6 Global Healthcare IoT Security Market Share, By Application, 2020
Figure 7 Global Healthcare IoT Security Market Share, By Region, 2020
Figure 8 North America: Global Healthcare IoT Security Market Share, By Country, 2020
Figure 9 Europe: Global Healthcare IoT Security Market Share, By Country, 2020
Figure 10 Asia-Pacific: Global Healthcare IoT Security Market Share, By Country, 2020
Figure 11 Middle East & Africa: Global Healthcare IoT Security Market Share, By Country, 2020
Figure 12 Global Healthcare IoT Security Market: Company Share Analysis, 2020 (%)
Figure 13 Inside Secure SA: Key Financials
Figure 14 Inside Secure SA: Segmental Revenue
Figure 15 Inside Secure SA: Geographical Revenue
Figure 16 IBM Corporation
Figure 17 Cisco Systems Inc.
Figure 18 Intel Corporation
Figure 19 Oracle Corporation
Figure 20 Sophos Group Plc
Figure 21 Symantec Corporation
Figure 22 Trend Micro Inc.
Figure 23 Checkpoint Software Technology
Figure 24 Kaspersky Labs
Figure 25 Fortinet Inc.
Figure 26 Intelen Inc.
Figure 27 Eurotech SpA
Figure 28 Deutsche Telekom AG
Figure 29 SecureFLO LLC
Figure 30 Dell Corporation
Figure 31 Atmel Corporation
Figure 32 Security Mentor
Figure 33 Klynveld Peat Marwick Goerdeler
Figure 34 Agile Cyber Security Solutions, LLC