

Threat Hunting Market Forecasts to 2030 – Global Analysis By Offering (Tool and Service), Threat Type (Advanced Persistent Threats (APTs), Malware and Ransomware, Insider Threats, Phishing and Social Engineering, DDoS, Zero-Day Exploits and Other Threat Types), Enterprise Size, Deployment Mode, End User and By Geography

<https://marketpublishers.com/r/T50AB81DB922EN.html>

Date: February 2025

Pages: 150

Price: US\$ 4,150.00 (Single User License)

ID: T50AB81DB922EN

Abstracts

According to Statistics MRC, the Global Threat Hunting Market is accounted for \$3.52 billion in 2024 and is expected to reach \$8.98 billion by 2030 growing at a CAGR of 16.9% during the forecast period. Threat hunting is a proactive approach to cybersecurity that aims to find and eliminate possible threats before they have a chance to do serious harm. Threat hunting is the process of actively looking for indications of malicious activity within a network or system, as opposed to traditional security measures that rely. Professionals in cybersecurity, also known as threat hunters, use a variety of instruments, methods, and data analytics to find irregularities, weaknesses, or indicators of compromise (IOCs). Threat hunting helps organizations stay ahead of cybercriminals and enhances the overall security posture by continuously examining patterns and behaviours.

According to a 2019 survey by the SANS Institute, 61% of respondents reported at least an 11% measurable improvement in their overall security posture after implementing threat hunting practices.

Market Dynamics:

Driver:

Growing cyber attacks and data breach incidents

Data breaches have grown to be a major worry for businesses in all industries. Concern over the necessity of strong cybersecurity systems has increased as a result of high-profile events like the Target, Equifax, and Colonial Pipeline hacks. Businesses are spending more money on threat-hunting capabilities since these breaches frequently lead to large financial losses, legal issues, and eroded trust. Additionally, lessening the overall impact and preventing hackers from gaining continuous access to sensitive systems and data, these solutions assist organizations in detecting breaches earlier.

Restraint:

Expensive implementation price

The high expense of implementing threat-hunting solutions is one of the main obstacles that organizations must overcome. Investing in specialized software tools, security infrastructure, and qualified staff is necessary to implement a successful threat-hunting program. Furthermore, there may be significant recurring operational expenses for things like threat-hunting, data analysis, and system maintenance. This expense might be unaffordable for small and medium-sized businesses (SMEs), which would restrict their capacity to adopt such cutting-edge cybersecurity measures.

Opportunity:

Developments in automated threat hunting

Automation in threat hunting is becoming increasingly important as cyber threats continue to grow in complexity. Organizations can scale their threat-hunting activities with automation while preserving accuracy and efficiency. Security staff is less burdened by automated systems' ability to continuously monitor network traffic, analyze massive datasets, and spot possible threats in real time. Additionally, automation can give early warnings of possible security breaches by assisting organizations in identifying threats that conventional methods might miss. Organizations have a great chance to take advantage of automated threat-hunting systems that improve their capacity to stop and address security incidents as automation technologies advance.

Threat:

Lack of qualified cybersecurity experts

A major obstacle to the market's expansion is the worldwide lack of qualified cybersecurity specialists, even in spite of the rising demand for threat-hunting solutions. Threat hunting is an extremely specialized field that necessitates a thorough comprehension of malware analysis, network behavior, and sophisticated threat detection techniques. However, there is a severe shortage of qualified personnel in the cybersecurity field who can efficiently manage these intricate programs. In furtherance of impeding the expansion of internal threat-hunting initiatives, this shortage makes businesses more dependent on managed services, which might not be a viable or long-term solution for all companies.

Covid-19 Impact:

The COVID-19 pandemic significantly impacted the threat hunting market by speeding up the transition to remote work and digital transformation, both of which raised the risk of cyber attacks. The attack surface grew as businesses quickly embraced remote access and cloud-based services to maintain business continuity, making threat detection and mitigation more difficult. The need for strong threat-hunting tactics was further underscored by the rise in cybercriminal activity, which included ransomware attacks, phishing campaigns, and data breaches. Moreover, the pandemic highlighted the lack of qualified experts and the increasing difficulty of protecting decentralized networks, even as it spurred increased investment in cybersecurity practices and tools, such as threat-hunting tools.

The Malware and Ransomware segment is expected to be the largest during the forecast period

The malware and ransomware segment is expected to account for the largest market share during the forecast period. With the growing sophistication of ransomware attacks, which have damaged operations and demanded large ransoms from organizations worldwide, these kinds of cyber threats have been on the rise. Since malware can spread quickly and cause serious harm, including data theft, system corruption, and unauthorized access, it remains a serious concern. Additionally, malware can take many different forms, including viruses, trojans, and spyware.

The Healthcare segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the healthcare segment is predicted to witness the highest growth rate. Healthcare organizations are more vulnerable to cyber attacks as they use digital technologies like telemedicine, electronic health records (EHR), and Internet of Things (IoT) devices. These attacks are especially likely to target sensitive patient data and vital healthcare infrastructure. Cybersecurity has become a top priority due to the increase in ransom ware attacks, data breaches, and the exploitation of healthcare systems. Furthermore, strong threat-hunting solutions are in greater demand as a result of the industry's quick digital transformation and strict legal requirements like HIPAA.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share. The region's power is fuelled by the existence of significant technology firms, sophisticated cybersecurity infrastructure, and a high concentration of big businesses that are progressively implementing threat-hunting solutions to defend vital systems and sensitive data against changing cyber threats. Increased investments in cybersecurity have been prompted by the notable increase in cyber attacks, including ransom ware, data breaches, and advanced persistent threats (APTs), in the United States in particular. Moreover, organizations are also being forced to give proactive threat-hunting tactics top priority by strict regulatory frameworks like the CCPA and GDPR.

Region with highest CAGR:

Over the forecast period, the Asia Pacific (APAC) region is anticipated to exhibit the highest CAGR. The region's attack surface for cyber threats has been greatly expanded by the rapid digital transformation of nations like China, India, Japan, and Southeast Asia, as well as the growing adoption of cloud, IoT, and mobile platforms. Additionally, the rise in cybercrime activities, such as ransom ware attacks, phishing, and data breaches, has led to organizations investing heavily in threat-hunting solutions, and governments in the region are stepping up efforts to improve cybersecurity capabilities through stricter laws and frameworks, which is propelling market growth.

Key players in the market

Some of the key players in Threat Hunting market include Broadcom, Inc., IBM Corporation, Palo Alto Networks, Inc., Check Point Software Technologies Ltd., Symantec, Rapid 7, Verizon Inc, Mindpoint Group, Capgemini, SentinelOne, Inc., Talatek, Sumo Logic, Inc., Cisco Systems, Inc., VMware Inc and CrowdStrike, Inc.

Key Developments:

In November 2024, Broadcom Inc. and Telia Company announced the expansion of their longtime partnership with a new multi-year agreement, which will see Telia further modernize and transform its telco and cloud infrastructure with the VMware product portfolio.

In July 2024, IBM announced that it has secured a five-year contract with \$26 million in initial funding from the U.S. Agency for International Development (USAID) to support its Cybersecurity Protection and Response (CPR) program aimed to expand and enhance the agency's cybersecurity response support for host governments in the Europe and Eurasia (E&E) region.

In May 2024, Palo Alto Networks and IBM unveiled a broad-reaching strategic partnership to strengthen each company's cybersecurity footprint in a move that promises to reshape the cybersecurity landscape. The wide-ranging agreement sees Palo Alto Networks acquiring IBM's QRadar SaaS business and incorporating IBM's watsonx LLMs into its Cortex XSIAM solution.

Offerings Covered:

Tool

Service

Threat Types Covered:

Advanced Persistent Threats (APTs)

Malware and Ransomware

Insider Threats

Phishing and Social Engineering

DDoS

Zero-Day Exploits

Other Threat Types

Enterprise Sizes Covered:

Small and Mid-Sized Enterprises (SMEs)

Large Enterprises

Deployment Modes Covered:

Cloud

On-Premises

End Users Covered:

Banking, Financial Services, and Insurance (BFSI)

IT and ITeS

Government

Energy and Utilities

Manufacturing

Healthcare

Retail & Ecommerce

Others End Users

Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2022, 2023, 2024, 2026, and 2030
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

1 EXECUTIVE SUMMARY

2 PREFACE

- 2.1 Abstract
- 2.2 Stake Holders
- 2.3 Research Scope
- 2.4 Research Methodology
 - 2.4.1 Data Mining
 - 2.4.2 Data Analysis
 - 2.4.3 Data Validation
 - 2.4.4 Research Approach
- 2.5 Research Sources
 - 2.5.1 Primary Research Sources
 - 2.5.2 Secondary Research Sources
 - 2.5.3 Assumptions

3 MARKET TREND ANALYSIS

- 3.1 Introduction
- 3.2 Drivers
- 3.3 Restraints
- 3.4 Opportunities
- 3.5 Threats
- 3.6 End User Analysis
- 3.7 Emerging Markets
- 3.8 Impact of Covid-19

4 PORTERS FIVE FORCE ANALYSIS

- 4.1 Bargaining power of suppliers
- 4.2 Bargaining power of buyers
- 4.3 Threat of substitutes
- 4.4 Threat of new entrants
- 4.5 Competitive rivalry

5 GLOBAL THREAT HUNTING MARKET, BY OFFERING

Threat Hunting Market Forecasts to 2030 – Global Analysis By Offering (Tool and Service), Threat Type (Advance...

5.1 Introduction

5.2 Tool

5.2.1 Endpoint Detection & Response (EDR)

5.2.2 Security Information and Event Management (SIEM)

5.2.3 Network Detection and Response

5.2.4 Other Tools

5.3 Service

5.3.1 Threat Hunting Services

5.3.2 Security Consulting

5.3.3 Integration & Implementation

5.3.4 Support Services

6 GLOBAL THREAT HUNTING MARKET, BY THREAT TYPE

6.1 Introduction

6.2 Advanced Persistent Threats (APTs)

6.3 Malware and Ransomware

6.4 Insider Threats

6.5 Phishing and Social Engineering

6.6 DDoS

6.7 Zero-Day Exploits

6.8 Other Threat Types

7 GLOBAL THREAT HUNTING MARKET, BY ENTERPRISE SIZE

7.1 Introduction

7.2 Small and Mid-Sized Enterprises (SMEs)

7.3 Large Enterprises

8 GLOBAL THREAT HUNTING MARKET, BY DEPLOYMENT MODE

8.1 Introduction

8.2 Cloud

8.3 On-Premises

9 GLOBAL THREAT HUNTING MARKET, BY END USER

9.1 Introduction

- 9.2 Banking, Financial Services, and Insurance (BFSI)
- 9.3 IT and ITeS
- 9.4 Government
- 9.5 Energy and Utilities
- 9.6 Manufacturing
- 9.7 Healthcare
- 9.8 Retail & Ecommerce
- 9.9 Others End Users

10 GLOBAL THREAT HUNTING MARKET, BY GEOGRAPHY

- 10.1 Introduction
- 10.2 North America
 - 10.2.1 US
 - 10.2.2 Canada
 - 10.2.3 Mexico
- 10.3 Europe
 - 10.3.1 Germany
 - 10.3.2 UK
 - 10.3.3 Italy
 - 10.3.4 France
 - 10.3.5 Spain
 - 10.3.6 Rest of Europe
- 10.4 Asia Pacific
 - 10.4.1 Japan
 - 10.4.2 China
 - 10.4.3 India
 - 10.4.4 Australia
 - 10.4.5 New Zealand
 - 10.4.6 South Korea
 - 10.4.7 Rest of Asia Pacific
- 10.5 South America
 - 10.5.1 Argentina
 - 10.5.2 Brazil
 - 10.5.3 Chile
 - 10.5.4 Rest of South America
- 10.6 Middle East & Africa
 - 10.6.1 Saudi Arabia
 - 10.6.2 UAE

- 10.6.3 Qatar
- 10.6.4 South Africa
- 10.6.5 Rest of Middle East & Africa

11 KEY DEVELOPMENTS

- 11.1 Agreements, Partnerships, Collaborations and Joint Ventures
- 11.2 Acquisitions & Mergers
- 11.3 New Product Launch
- 11.4 Expansions
- 11.5 Other Key Strategies

12 COMPANY PROFILING

- 12.1 Broadcom, Inc.
- 12.2 IBM Corporation
- 12.3 Palo Alto Networks, Inc.
- 12.4 Check Point Software Technologies Ltd.
- 12.5 Symantec
- 12.6 Rapid 7
- 12.7 Verizon Inc
- 12.8 Mindpoint Group
- 12.9 Capgemini
- 12.10 SentinelOne, Inc.
- 12.11 Talatek
- 12.12 Sumo Logic, Inc.
- 12.13 Cisco Systems, Inc.
- 12.14 VMware Inc
- 12.15 CrowdStrike, Inc.

List Of Tables

LIST OF TABLES

- Table 1 Global Threat Hunting Market Outlook, By Region (2022-2030) (\$MN)
- Table 2 Global Threat Hunting Market Outlook, By Offering (2022-2030) (\$MN)
- Table 3 Global Threat Hunting Market Outlook, By Tool (2022-2030) (\$MN)
- Table 4 Global Threat Hunting Market Outlook, By Endpoint Detection & Response (EDR) (2022-2030) (\$MN)
- Table 5 Global Threat Hunting Market Outlook, By Security Information and Event Management (SIEM) (2022-2030) (\$MN)
- Table 6 Global Threat Hunting Market Outlook, By Network Detection and Response (2022-2030) (\$MN)
- Table 7 Global Threat Hunting Market Outlook, By Other Tools (2022-2030) (\$MN)
- Table 8 Global Threat Hunting Market Outlook, By Service (2022-2030) (\$MN)
- Table 9 Global Threat Hunting Market Outlook, By Threat Hunting Services (2022-2030) (\$MN)
- Table 10 Global Threat Hunting Market Outlook, By Security Consulting (2022-2030) (\$MN)
- Table 11 Global Threat Hunting Market Outlook, By Integration & Implementation (2022-2030) (\$MN)
- Table 12 Global Threat Hunting Market Outlook, By Support Services (2022-2030) (\$MN)
- Table 13 Global Threat Hunting Market Outlook, By Threat Type (2022-2030) (\$MN)
- Table 14 Global Threat Hunting Market Outlook, By Advanced Persistent Threats (APTs) (2022-2030) (\$MN)
- Table 15 Global Threat Hunting Market Outlook, By Malware and Ransomware (2022-2030) (\$MN)
- Table 16 Global Threat Hunting Market Outlook, By Insider Threats (2022-2030) (\$MN)
- Table 17 Global Threat Hunting Market Outlook, By Phishing and Social Engineering (2022-2030) (\$MN)
- Table 18 Global Threat Hunting Market Outlook, By DDoS (2022-2030) (\$MN)
- Table 19 Global Threat Hunting Market Outlook, By Zero-Day Exploits (2022-2030) (\$MN)
- Table 20 Global Threat Hunting Market Outlook, By Other Threat Types (2022-2030) (\$MN)
- Table 21 Global Threat Hunting Market Outlook, By Enterprise Size (2022-2030) (\$MN)
- Table 22 Global Threat Hunting Market Outlook, By Small and Mid-Sized Enterprises (SMEs) (2022-2030) (\$MN)

Table 23 Global Threat Hunting Market Outlook, By Large Enterprises (2022-2030) (\$MN)

Table 24 Global Threat Hunting Market Outlook, By Deployment Mode (2022-2030) (\$MN)

Table 25 Global Threat Hunting Market Outlook, By Cloud (2022-2030) (\$MN)

Table 26 Global Threat Hunting Market Outlook, By On-Premises (2022-2030) (\$MN)

Table 27 Global Threat Hunting Market Outlook, By End User (2022-2030) (\$MN)

Table 28 Global Threat Hunting Market Outlook, By Banking, Financial Services, and Insurance (BFSI) (2022-2030) (\$MN)

Table 29 Global Threat Hunting Market Outlook, By IT and ITeS (2022-2030) (\$MN)

Table 30 Global Threat Hunting Market Outlook, By Government (2022-2030) (\$MN)

Table 31 Global Threat Hunting Market Outlook, By Energy and Utilities (2022-2030) (\$MN)

Table 32 Global Threat Hunting Market Outlook, By Manufacturing (2022-2030) (\$MN)

Table 33 Global Threat Hunting Market Outlook, By Healthcare (2022-2030) (\$MN)

Table 34 Global Threat Hunting Market Outlook, By Retail & Ecommerce (2022-2030) (\$MN)

Table 35 Global Threat Hunting Market Outlook, By Others End Users (2022-2030) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

I would like to order

Product name: Threat Hunting Market Forecasts to 2030 – Global Analysis By Offering (Tool and Service), Threat Type (Advanced Persistent Threats (APTs), Malware and Ransomware, Insider Threats, Phishing and Social Engineering, DDoS, Zero-Day Exploits and Other Threat Types), Enterprise Size, Deployment Mode, End User and By Geography

Product link: <https://marketpublishers.com/r/T50AB81DB922EN.html>

Price: US\$ 4,150.00 (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/T50AB81DB922EN.html>