

Ransomware Protection - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 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 Ransomware Protection Market size is estimated at USD 21.20 billion in 2024, and is expected to reach USD 51.73 billion by 2029, growing at a CAGR of 19.53% during the forecast period (2024-2029).

The global ransomware protection market is expanding due to rising company digitization, increased use of ransomware-as-a-service (RaaS), and the introduction of cryptocurrencies like Bitcoin. However, a lack of knowledge about cyberattacks and financial limitations limit business expansion. On the other hand, new opportunities will arise as enterprises seek more multi-layer security protection and cloud-based services are used more widely.

Key Highlights

-Owing to the increase in the demand for ransomware protection in recent years as a service, the global ransomware protection market is projected to witness a significant growth rate. The advent of cryptocurrencies, such as Bitcoin, Ethereum, increased the demand for ransomware protection solutions as a majority of the ransom is demanded in the form of cryptocurrency due to its untraceable nature. Moreover, the industry is impacted by technological developments and has seen the advent of ransomware protection solutions for mobile devices, too, apart from PCs.

-Moreover, the evolution of ransomware tactics, techniques, and procedures (TTPs) has heightened the need for advanced protection mechanisms. Ransomware-as-a-Service (RaaS) models, polymorphic malware, and targeted attacks on critical infrastructure have become prevalent, necessitating adaptive and sophisticated defense solutions. The ransomware protection market responds to these challenges by offering comprehensive cybersecurity suites that include threat intelligence, endpoint protection, network security, and data backup and recovery.

-Also, companies are nearly three times more susceptible to suffering breaches through social attacks than via actual vulnerabilities, emphasizing the need for ongoing employee cybersecurity education. It has led to the company looking towards

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scott-international.com

www.scott-international.com

ransomware protection solutions and has provided a considerable push for the solutions demand in the studied market.

-Worldwide, a rise in ransomware attacks was brought on by the global COVID-19 outbreak. For many years, ransomware has been the assault strategy of choice for online thieves. Organizations witnessed an increase in the size and sophistication of these attacks. According to Interpol, COVID-19 drastically changed the dangerous environment from attacks on people and small companies to essential infrastructure, governments, and large organizations.

Ransomware Protection Market Trends

Cloud Deployment Plays a Major Role in Ransomware Protection

- Cloud storage is not resistant to ransomware threats and is not foolproof. Ransomware can certainly affect cloud storage, especially if the cloud storage dealers are not proactively using anti-ransomware technology. In fact, ransomware can impact any and all internet-connected strategies. This includes IoT devices, like security thermostats, cameras, doorbells, and others like PCs, file, email, and data servers, and cloud-based servers, which performs as cloud storage.

- Cloud storage vendors should constantly be evaluating, testing, and upgrading their security solutions and using multilayered defense methods. Organizations should ask merchants to share their precise and specific ransomware detection, quarantine, and removal procedures.

- Organizations can also deploy anti-ransomware protection software on all devices, including cloud servers and cloud storage. That software should have redundancy and failover defense in case of a ransomware attack. Organizations are also required to have data backup and retrieval policies and plans that are really implemented and practiced. And (they should) conduct ongoing backups of all data as part of those disaster retrieval policies.

- Further, it depends on sound design and architecture rather than intrusion detection and security analysis, security in the cloud is unique. Hackers attempt to take advantage of cloud misconfigurations that allow them to operate against your cloud control plane APIs and steal data out from under rather than breaking into the network to lock out of systems.

North America Holds The Largest Market Share in Ransomware Protection Market

- The region is known for infiltration and cyber-attacks. For instance, the SamSam ransomware was used to attack Atlanta's IT infrastructure by infiltrating into the network, hiding its presence while it harvested credentials to spread to multiple computers before locking them up. It resulted in a mass shutdown of online city services and an estimated cost of at least USD 2.6 million in clean-up and response.

- Further, in September 2023, The FBI is warning businesses in the United States to be on the lookout for dual ransomware attacks, in which the same organization is targeted more than once in quick succession. The FBI also stated that a variety of ransomware tools are being used in various combinations, with potentially disastrous consequences for targeted businesses. "The use of dual ransomware variants resulted in data encryption, exfiltration, and financial losses as a result of ransom payments.

- There is a continued rise in the threats from other nations which try to affect the critical infrastructure of the US, WannaCry was one such target ransomware where Park Jin-hook, a North Korean national, was charged for being part of a WannaCry attack undertaken on behalf of the North Korean government. Such actions have pushed organizations to improve the security segment and strengthen their IT security by updating the services.

- Moreover, in November 2023, Malwarebytes, a company that provides real-time cyber protection, announced the launch of ThreatDown, a product family that provides effective, easy-to-use cybersecurity to IT-constrained organizations.

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

The ransomware protection market consists of several players. In terms of market share, few of the players currently dominate the market. These major players with a prominent share of the market are focusing on expanding their customer base across foreign countries. These companies are leveraging strategic collaborative initiatives to increase their market share and increase their profitability.

- In January 2023 - A pre-existing alliance between chipmaker Intel and cybersecurity firm Check Point Software Technologies was extended to offer hardware-level defense against ransomware, one of the most common security dangers of the present.
- In June 2023 - CTERA announced the release of CTERA Ransom Protect, a new AI-powered cyber protection engine integrated into the CTERA global file system. CTERA Ransom Protect detects and blocks attacks in seconds, thanks to activity sensors built into the file system that feed an advanced machine learning algorithm trained on a large dataset of attack flows. It also provides tools for immediate mitigation and recovery.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION

- 1.1 Market Definition and Scope
- 1.2 Study Assumptions

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS

- 4.1 Market Overview
- 4.2 Industry Stakeholder Analysis
- 4.3 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.3.1 Bargaining Power of Suppliers
 - 4.3.2 Bargaining Power of Consumers
 - 4.3.3 Threat of New Entrants
 - 4.3.4 Threat of Substitute Products
 - 4.3.5 Intensity of Competitive Rivalry

5 MARKET DYNAMICS

- 5.1 Market Overview
- 5.2 Market Drivers
 - 5.2.1 Increasing Number of Phishing Attacks and Targeted Security Breaches
 - 5.2.2 Emergence of Ransomware as a Service Model
 - 5.2.3 Use of Crypto Currencies as Payment Method
 - 5.2.4 Cloud Deployment Plays a Major Role in Ransomware Protection

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

5.3 Market Restraints

5.3.1 Availability of Free Endpoint Solutions for Ransomware Protection

6 MARKET SEGMENTATION

6.1 Deployment

6.1.1 On-Premise

6.1.2 On-Cloud

6.2 Application

6.2.1 Endpoint Protection

6.2.2 Email Protection

6.2.3 Network Security

6.2.4 Other Applications

6.3 Geography

6.3.1 North America

6.3.1.1 United States

6.3.1.2 Canada

6.3.2 Europe

6.3.2.1 Germany

6.3.2.2 UK

6.3.2.3 France

6.3.2.4 Spain

6.3.2.5 Rest of Europe

6.3.3 Asia-Pacific

6.3.3.1 China

6.3.3.2 Japan

6.3.3.3 India

6.3.3.4 Australia

6.3.3.5 Rest of Asia-Pacific

6.3.4 Latin America

6.3.4.1 Brazil

6.3.4.2 Mexico

6.3.4.3 Argentina

6.3.4.4 Rest of Latin America

6.3.5 Middle East and Africa

6.3.5.1 UAE

6.3.5.2 Saudi Arabia

6.3.5.3 South Africa

6.3.5.4 Rest of Middle East and Africa

7 COMPETITIVE LANDSCAPE

7.1 Company Profiles*

7.1.1 McAfee, LLC

7.1.2 AO Kaspersky Lab

7.1.3 Bitdefender

7.1.4 FireEye, Inc.

7.1.5 Malwarebytes

7.1.6 SentinelOne

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 7.1.7 Sophos Ltd.
- 7.1.8 Symantec Corporation
- 7.1.9 Trend Micro Incorporated
- 7.1.10 Zscaler, Inc

8 INVESTMENT ANALYSIS

9 MARKET OPPORTUNITIES AND FUTURE TRENDS

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

**Ransomware Protection - Market Share Analysis, Industry Trends & Statistics,
Growth Forecasts 2019 - 2029**

Market Report | 2024-02-17 | 120 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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-02"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

