

Global Content Disarm and Reconstruction - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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 Global Content Disarm and Reconstruction Market is expected to register a CAGR of 14% during the forecast period.

Key Highlights

- The ransomware damages are predicted to reach a global number of USD 15-16 billion in 2021, up many times from the global damages it achieved in 2015, which was around USD 260 million. Owing to such a rapid increase in attacks, the market witnessed a record influx of capital by investors into more than 1,000 deals, of which 84 were more significant than USD 100 million.
- The Momentum Cyber also suggested that these transactions included a USD 200 million Series D investment secured by industrial cybersecurity startup Dragos, Claroty's USD 140 million pre-IPO raise, and the USD 543 million Series A raised by passwordless authentication company Transmit Security. Additionally, the total financing value was 138% over the previous year. As a result of this historic investment volume, a record number of security startups were minted as unicorns in 2021. More than 30 startups achieved USD 1 billion-plus valuations, including Wiz, Noname Security, and LaceWork, compared to just six startups the previous year.
- The market is expected to rise due to the rising acceptance of cloud-based security solutions, increased awareness of security threats, and the developing of cybersecurity solutions for connected IoT devices. Furthermore, shifting IT trends and the increasing adoption of cloud solutions are opening potential growth prospects for content disarm and reconstruction solutions, which are utilized to protect an organization's data, brand value, and identity.
- Furthermore, with implementing the general data protection regulation (GDPR) to help combat persistent security leaks of sensitive personal information, governments and regulatory bodies are increasingly expecting more robust compliance and regulation norms for content security. The demand for content disarm, and reconstruction solutions are growing as governments across the globe spend extensively on digitalization and the transformation of IT infrastructure.
- Further, Swissinfo.ch stated that the NCSC (National Cyber Security Center) reported 350 cyberattacks (phishing, fake websites,

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

direct attacks on organizations, etc.), compared to 100-150 occurrences. The increase in working from home was attributed to the coronavirus pandemic, as persons working at home lack the same intrinsic protection and deterrent measures as those in a working environment (e.g., internet security). The threat of such breaches will create lucrative opportunities for the global content disarm and reconstruction market to prevent malicious attackers from entering the network perimeter.

Content Disarm and Reconstruction Market Trends

SMEs Segment to Grow at a Higher Pace During the Forecast Period

- The SME segment is anticipated to grow at a higher CAGR during the forecast period due to the growing data protection regulations and scarcity of high-cost security solutions within the network infrastructure. SMEs are small in terms of size but cater to a vast number of clients globally. The robust and comprehensive content disarm, and reconstruction solution is not implemented in SMEs due to financial constraints in these organizations. Weak cybersecurity and low budget make SMEs more susceptible to data breaches and identity thefts.
- The cloud deployment mode is expected to grow at a higher CAGR as Small and Medium-sized Enterprises (SMEs) quickly adopt the cost-effective cloud deployment model. There is an increasing trend of PaaS and IaaS among SMBs for consumer cloud services, file sharing, CRM, email, chat, and internal communication. While retaining the on-premise network, SMBs are more willing to integrate the cloud into their network infrastructure as they adopt new technologies.
- Overall, SMBs have great opportunities to adopt effective strategies to stand in the competition, and the cloud has a vital role in the process. For instance, a recent study done by Microsoft surveyed more than 3,000 SMEs across 16 countries to understand whether SMEs have an appetite for adopting Cloud computing. One of the findings was that within three years, the workloads of 43 % would become paid Cloud services.
- Cloud Solutions offers a gamut of advantages to small and medium business owners. With the scalability and flexibility of cloud solutions, one can quickly move forward by taking competitive advantages. For instance, Apogaeis Technologies LLP provides SaaS and PaaS solutions to many global SMEs and adds value to their entire business process.
- Moreover, in March 2021, Attacks on on-premise Microsoft Exchange servers have increased, according to security agencies. Small and medium-sized enterprises frequently use email servers. Therefore, these attacks were carried out on them. For these reasons, Microsoft has introduced a new one-click Mitigation Tool for clients with Microsoft Exchange servers on-premise. Customers who are inexperienced with the patch/update process will benefit from this.

North America to Account for the Largest Market Size

- North America is supposed to become the most significant revenue-generating area for content disarm, reconstruction solutions, and service vendors. The growing number of ransomware, APTs, zero-day attacks, and the mounting amount of malware and file-based attacks are some of the principal factors anticipated to feed the market growth in North America.
- North America includes major economies, such as the United States of America and Canada, quickly using the CDR solution. The CDR market in the region is getting traction as it gives proactive security measures for securing I.T. systems from malware. SMEs and large companies in the area have become highly aware of CDR services and have begun using them to fight cyber threats.
- To safeguard the interest of governments and private entities, various initiatives have been launched that are expected to draw the map for infrastructure cybersecurity over the coming years. For example, in March 2021, the United States announced its plans to launch three new research programs to protect the security of the country's energy system. The DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) announced new programs to help safeguard the U.S. energy system from increasing cyber and physical hazards. Such initiatives are expected to pave the way for adopting solutions in the

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

segment.

- Also, according to the United States Office of Management and Budget, for F.Y. 2021, the United States government proposed an 18.78 billion U.S. dollar budget for cybersecurity, supporting a broad-based cybersecurity strategy for securing the government and enhancing the security of critical infrastructure and essential technologies. California reported a loss of more than 573 million U.S. dollars through cybercrime, almost double the amount of second-placed New York, which said 293 million U.S. dollars of losses, says IC3.
- The North American market is attaining traction, as the content disarm and reconstruction solution gives proactive security means for stopping data breaches. SMEs and large regional organizations have become more conscious of the content disarm and reconstruction process and its advantages and started embracing them to fight cyber fraud and data thefts.

Content Disarm and Reconstruction Industry Overview

The Content Disarm and Reconstruction Market is moderately competitive and consists of several key players. Significant vendors who offer services across the globe are Check Point Software Technologies, Fortinet, Deep Secure, Sasa Software, ReSec Technologies, and OPSWAT, among others. These vendors have adopted various organic and inorganic growth strategies, such as new product launches, partnerships, collaborations, and acquisitions, to expand their offerings in the content disarm and reconstruction market.

- July 2022: OPSWAT, cybersecurity and CDR solutions for critical infrastructure protection (CIP), announced that it had attained the Amazon Web Services (AWS) Security Competency in the data protection category. This accreditation acknowledges that OPSWAT has proven that it can provide clients with cybersecurity expertise in Data Protection to assist them in achieving their cloud security objectives and has successfully met AWS's technical and quality requirements.
- March 2022: Glasswall, a provider of Content Disarm and Reconstruction (CDR) technology, recently made its market-dominating desktop CDR tool available in a freemium version called Glasswall Desktop Freedom. It provides protection that doesn't wait for detection so that users can trust every file. This technology was developed to assist safeguard organizations in the public and private sectors from the hazards of file-based attacks like malware and ransomware. Users have access to the freemium edition for 12 months after the date of their original download.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION

1.1 Study Assumptions and Market Definition

1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET DYNAMICS

4.1 Market Overview

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

4.2 Market Drivers

4.2.1 Growing Number of Ransomware, Apts, and Zero-Day Attacks

4.2.2 Augmented Stringent Regulations and Compliances

4.2.3 Rising Number of Malware and File-Based Attacks

4.3 Market Restraints

4.3.1 Budgetary Obstacles in Deploying Content Disarm and Reconstruction Solutions

4.4 Industry Attractiveness - Porter's Five Forces Analysis

4.4.1 Bargaining Power of Suppliers

4.4.2 Bargaining Power of Consumers

4.4.3 Threat of New Entrants

4.4.4 Threat of Substitutes

4.4.5 Intensity of Competitive Rivalry

4.5 Assessment of Impact of COVID-19 on the Industry

5 MARKET SEGMENTATION

5.1 By Component

5.1.1 Solutions

5.1.2 Services

5.2 By Deployment Mode

5.2.1 On-Premises

5.2.2 Cloud

5.3 By Application Area

5.3.1 Email

5.3.2 Web

5.3.3 File Transfer Protocol

5.3.4 Other Application Areas

5.4 By Organization Size

5.4.1 Small and Medium-Sized Enterprises

5.4.2 Large Enterprises

5.5 By End-user Vertical

5.5.1 BFSI

5.5.2 IT and Telecom

5.5.3 Government

5.5.4 Manufacturing

5.5.5 Healthcare

5.5.6 Other End-user Verticals

5.6 By Geography

5.6.1 North America

5.6.2 Europe

5.6.3 Asia Pacific

5.6.4 Latin America

5.6.5 Middle East and Africa

6 COMPETITIVE LANDSCAPE

6.1 Company Profiles

6.1.1 Fortinet, Inc.

6.1.2 Check Point Software Technologies

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- 6.1.3 OPSWAT, Inc.
- 6.1.4 Deep Secure Inc.
- 6.1.5 Re-Sec Technologies Ltd.
- 6.1.6 Votiro Inc.
- 6.1.7 Glasswall Solutions Limited
- 6.1.8 Sasa Software (CAS) Ltd.
- 6.1.9 Peraton Corporation
- 6.1.10 YazamTech Inc.
- 6.1.11 Jiransecurity Ltd.
- 6.1.12 Mimecast Services limited.
- 6.1.13 SoftCamp Co., Ltd.
- 6.1.14 Cybace Solutions

7 INVESTMENT ANALYSIS

8 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

Global Content Disarm and Reconstruction - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-05
		Signature	

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com



Scotts International. EU Vat number: PL 6772247784

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