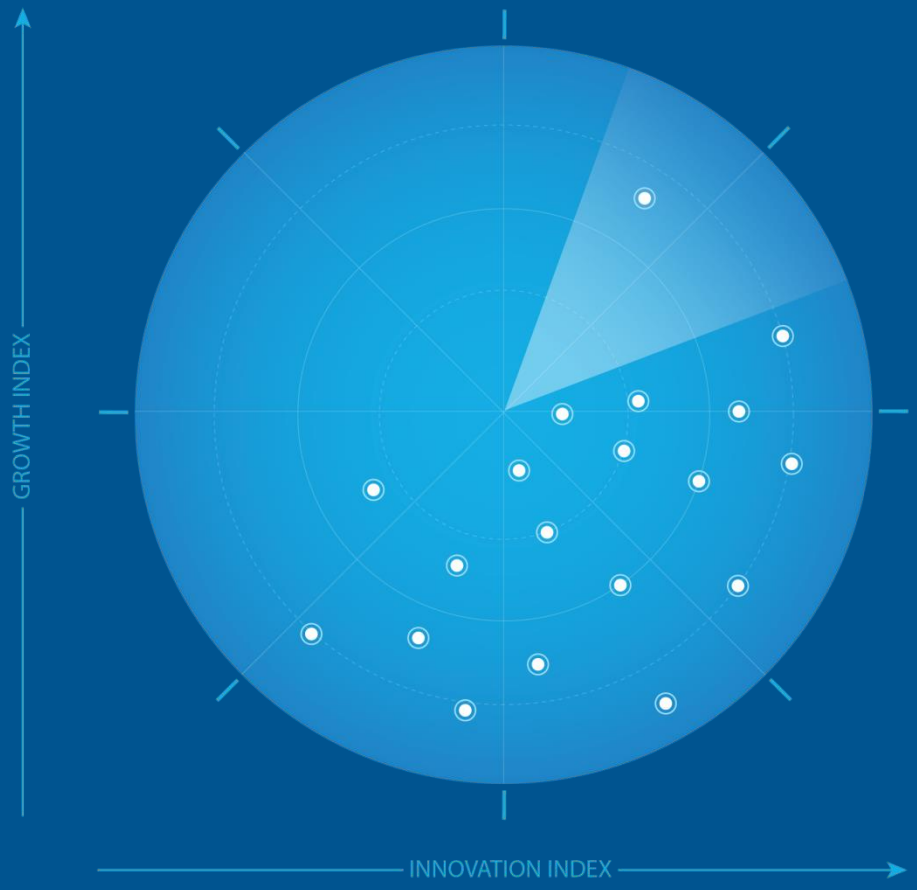
FROST & SULLIVAN

Frost Radar™: Digital Risk Protection (DRP) Services, 2022

A Benchmarking System to Spark Companies to Action—Innovation that Fuels New Deal Flow and Growth Pipelines



Global Security Research Team at Frost & Sullivan

K7CF-74
December 2022

FROST & SULLIVAN

Strategic Imperative and Growth Environment

The Strategic Imperative

- Demand for digital risk protection (DRP) solutions has skyrocketed as cyberattacks targeting organizations' brand equity, customers, and employees are on the rise.
- The COVID-19 pandemic has accelerated the shift to remote work environments and caused many organizations to rush their digital transformation initiatives, such as cloud migration, leading to increased risk to and exposure of their digital assets. In addition, the lines between work and personal devices have blurred, which changed the traditional security perimeter, making it more difficult for legacy security solutions to protect an enterprise's digital assets.
- With the help of sophisticated artificial intelligence/machine learning (AI/ML) algorithms, hackers have been launching new targeted phishing campaigns on a large scale by imitating an organization's external digital assets, such as websites, mobile apps, and social media accounts. As organizations conduct more business and personal interactions virtually, the risk of customers and employees falling victim to a phishing attack that impersonates a company brand or executive has increased significantly.
- The dynamic nature of the threat landscape and the vast number of resources it takes to monitor, analyze, and mitigate phishing attempts effectively make it impossible for organizations to protect their external attack surface without the help of a designated DRP platform.
- A successful phishing attack can have devastating consequences, including brand erosion, business disruption, and considerable financial losses. As a result, more organizations prioritize protecting their external attack surface beyond the corporate firewall.

Source: Frost & Sullivan

The Strategic Imperative (continued)

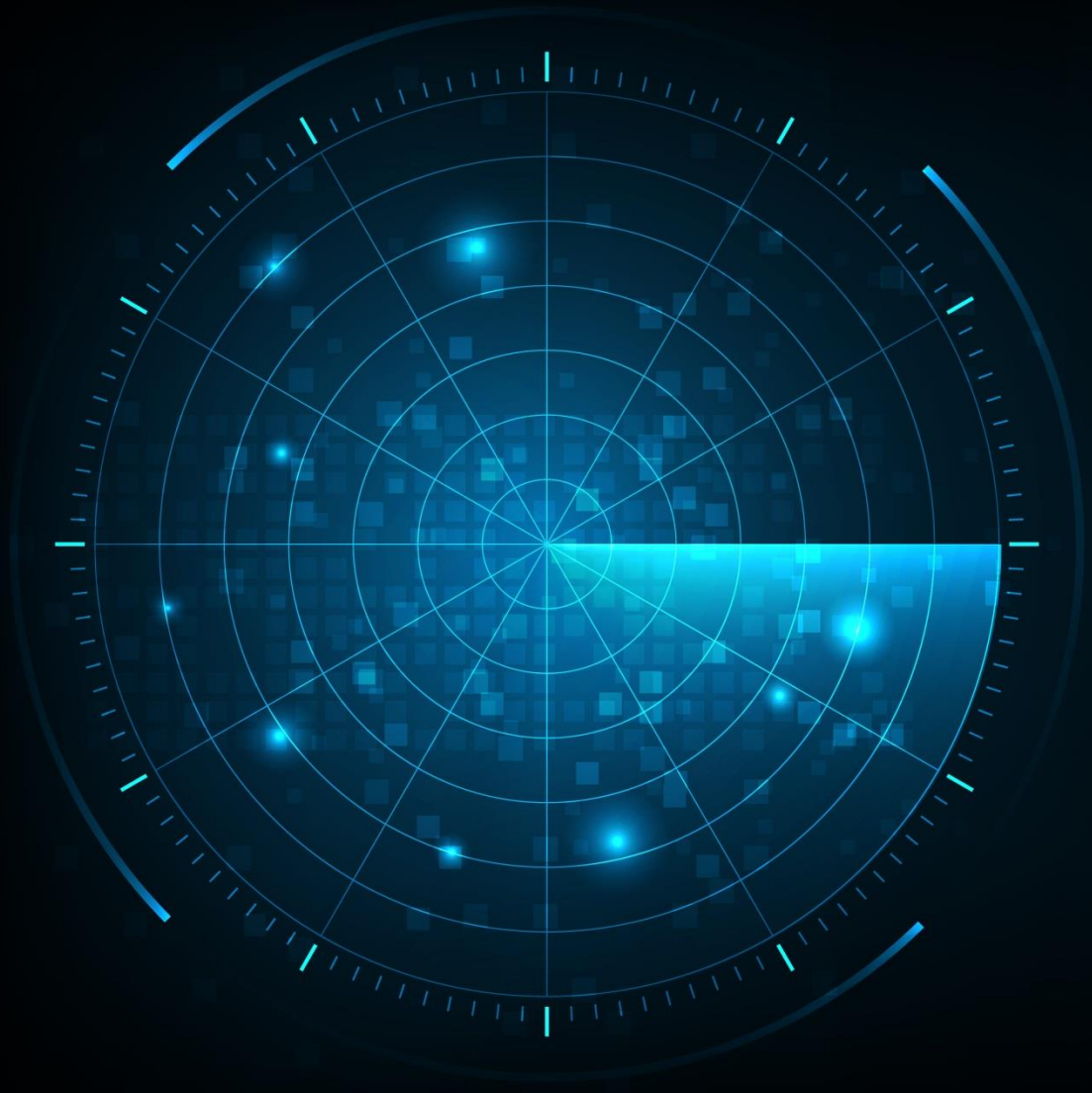
- As the rise of new cyberthreats and the greater risk of being attacked on the external digital surface have boosted demand for DRP products, more vendors from adjacent cybersecurity fields are now offering their own DRP use cases.
- In addition, the cybersecurity market is converging as many vendors offer a broad suite of products, including DRP, email security, network security, and extended detection and response (XDR). Specifically, cybersecurity vendors are consolidating CTI, EASM, and DRP capabilities to offer organizations a holistic security posture for their digital footprint.
- Cybersecurity consolidation and the emergence of ERMM platforms will negatively impact DRP point solution providers as well as hinder and limit their growth potential in the next five years. Due to the highly dynamic nature of phishing and brand impersonation threats, organizations require a multi-layered cybersecurity posture, which conventional DRP solutions will not be able to provide, unless they are complemented by EASM, CTI, and third-party risk assessment capabilities.
- As enterprise customers prefer to buy from fewer vendors, Frost & Sullivan expects more pure-play DRP providers to offer additional services packaged as one managed subscription during the next five years.
- Last, the ongoing Russo-Ukrainian War and the European energy crisis are causing supply chain disruptions, economic decline, and rising energy costs, which subsequently may limit organizations' cybersecurity budgets and force them to reprioritize business spending.

Source: Frost & Sullivan

The Growth Environment

- The global DRP market on a high growth trajectory, increasing at compound annual growth rate (CAGR) of 39.7% from 2021 to 2026. Frost & Sullivan expects it to reach $917.7 million by 2026.
- Of the $172.5 million total market revenue in 2021, DRP services vendors generated 41.7% while ERMM vendors generated 58.3%.
- In its early stage, the DRP market is undersaturated, leaving much room for growth. However, DRP vendors (DRP services and ERMM providers) continue prioritizing development in the Europe, Middle East, and Africa (EMEA) and North American regions.
- The DRP market is experiencing an influx of new competitors as cybersecurity vendors from adjacent fields, such as CTI, have adopted DRP use cases.
- Larger enterprises from the finance, technology, and retail industries are the target markets for DRP vendors, although small-to-medium businesses are experiencing higher adoption rates.
- Critical growth drivers include the increasing number of phishing attacks, rapid digitalization efforts, industry convergence, changes in cybersecurity spending, and regulatory compliance frameworks.
- Some notable growth restraints are increased competition, low prioritization of DRP (thus limited cybersecurity budget), technological restrictions, and limited awareness of DRP.
- Frost & Sullivan studies related to this independent analysis:
  - European Digital Risk Protection (DRP) Market, Forecast to 2024
  - Frost Radar: European Digital Risk Protection (DRP) Market, 2020
  - Global Digital Risk Protection (DRP) Market, Forecast to 2026
  - Frost Radar: External Risk Mitigation and Management (ERMM) Platforms, 2022 (upcoming)

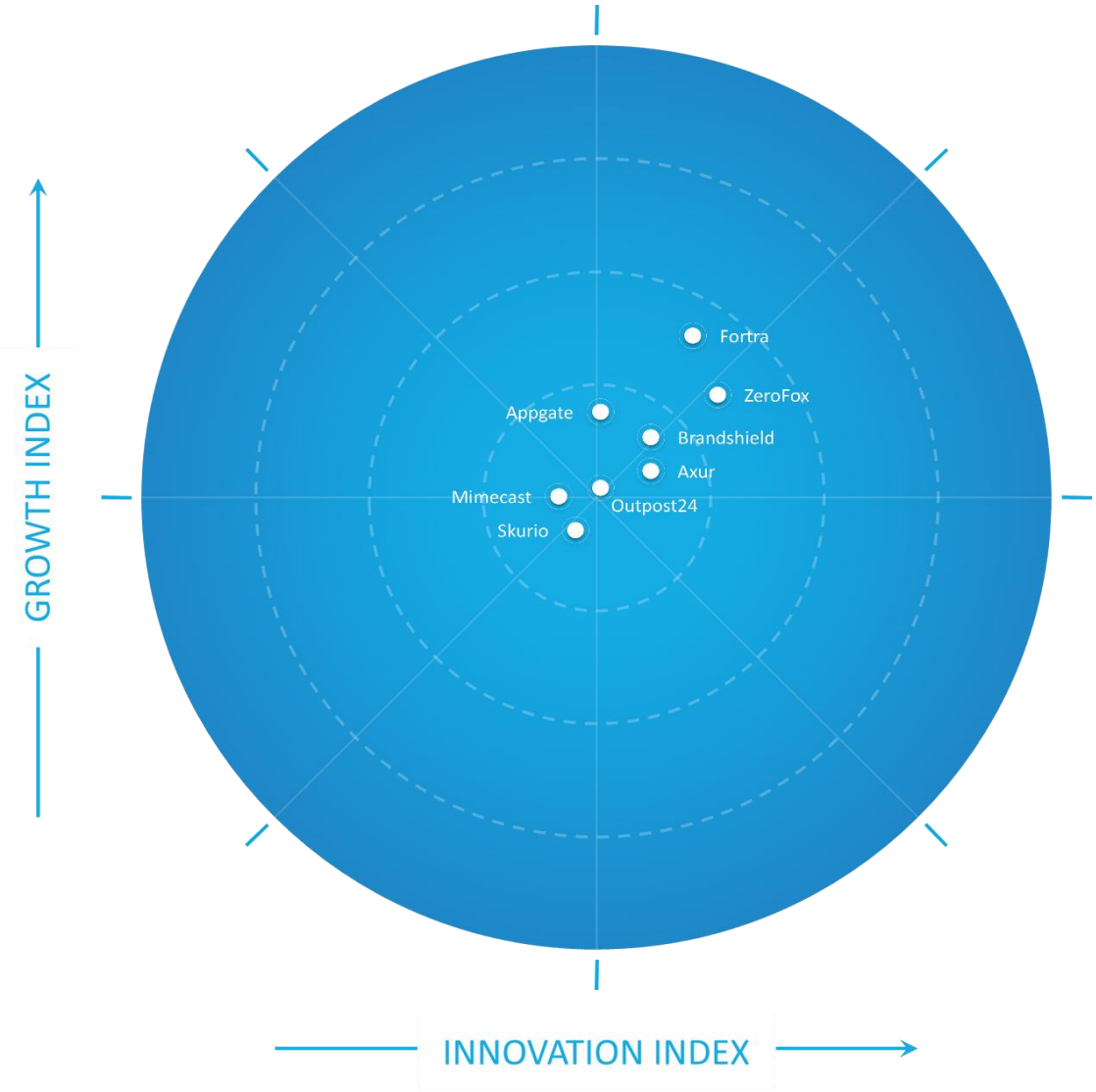
Source: Frost & Sullivan



Frost Radar™

DRP Services

Frost Radar™: DRP Services*



*Fortinet and Mandiant entered the market mid-year and therefore are not reflected in this Frost Radar.

Source: Frost & Sullivan

Frost Radar™: Competitive Environment

- The global DRP market is highly competitive, dynamic, and fragmented, as it is still in its adolescent stage, allowing vendors to build out their niches without directly impacting each other's revenue growth. As a result, vendors have no more than 10% share of the total global market revenue, with two exceptions.
- In a field of more than 20 industry participants, Frost & Sullivan independently plotted the top 8 DRP service providers in this Frost Radar™ analysis. While more market participants are either exploring or entering the DRP market, Frost & Sullivan has identified these 8 vendors as established participants with significant market share.
- Some vendors, including Appgate, Outpost24, and Mimecast, have entered the DRP space from adjacent markets, such as security information and event management (SIEM), email security, and CTI.
- ZeroFox is leading the Innovation Index due to its numerous DRP use cases, research, and development investments.
- Fortra is the Growth Index frontrunner with its market share, strategic sales, and marketing initiatives.
- Fortinet and Mandiant entered the DRP space in June 2022, illustrating rapid growth within the first quarter; however, these vendors are not benchmarked in this report.
- Axur, Brandshield, and Skurio offer great brand protection and threat intelligence capabilities, filling out individual niches in their respective markets, such as Latin America and Europe.

Source: Frost & Sullivan

FROST & SULLIVAN

Companies to Action

Companies to Be Considered First for Investment, Partnerships, or Benchmarking

Brandshield

INNOVATION

- Brandshield offers a wide range of DRP use cases and specializes in monitoring, detecting, and removing phishing attacks, including brand and executive impersonation.
- The DRP vendor's unique value proposition lies in its in-depth brand protection capabilities, such as trademark and counterfeit infringement, executive impersonation, and paid ad monitoring.
- Brand protection is no longer just a cybersecurity issue. Brandshield's intuitive user interface (UI) enables legal, marketing, and cybersecurity teams to collaborate more efficiently and mitigate brand impersonation attempts on all forefronts.

GROWTH

- Headquartered in Herzliya, Israel, Brandshield primarily targeted large and mid-size enterprises in the North American market's consumer products, financial, and healthcare sectors.
- Brandshield experienced steady growth rates in the past three years and continues to expand its market presence, mainly via its direct sales and online channels.
- With the DRP platform's refinement, Brandshield is now looking to expand its North American market share in new industry verticals, such as gaming and blockchain, through new sales and marketing initiatives.

FROST PERSPECTIVE

- Brandshield focuses its DRP services on the North American region. Although the DRP market is still a greenfield, the vendor must consider expanding into the EMEA region, where numerous enterprises have advanced security maturity.
- Although the company has generated most of its revenue through its direct sales channel, it is vital for Brandshield to expand its partner network through resellers and MSSPs, which will enable growth in the EMEA and other regions.

Source: Frost & Sullivan

FROST & SULLIVAN

Strategic Insights

Strategic Insights

1

An organization's ability to monitor its external attack surface in real-time and automatically take down fraudulent websites within minutes of discovery is growing in importance. However, the effectiveness of DRP solutions depends on various factors, such as the range of digital assets monitored, the sophistication of ML/AI analysis tools, the type of remediation services provided, and workflow automation capabilities. A few examples of how vendors differentiate their DRP services are the mean time for remediation, takedown success rate, and the number of takedowns offered.

2

The global DRP market is rapidly changing and becoming more competitive as vendors from adjacent cybersecurity fields, such as email security, network security, CTI, and EASM, offer their own DRP use cases. In addition, due to the high overlap between CTI, EASM, and DRP, many vendors are consolidating their services into an integrated ERMM platform. As a result, Frost & Sullivan expects more DRP vendors to follow suit and combine CTI, EASM, and DRP use cases to stay ahead of the competition.

3

Most DRP vendors focus on one specific region, which limits their revenue potential. While the DRP market is still a greenfield with substantial room for growth, vendors should capitalize on geographic expansion. North America and the EMEA regions are similar in market size, security maturity, and enterprise concentrations. Therefore, vendors focused on North America should look to EMEA as the most accessible opportunity, and vice-versa. In addition, vendors should consider partnering with local resellers and MSSPs to expand their operations in different industries and geographies.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

VERTICAL AXIS

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline™ system; and effective market, competitor, and end-user focused sales and marketing strategies.

GROWTH INDEX ELEMENTS

- **GI1: MARKET SHARE (PREVIOUS 3 YEARS)**
  This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.
- **GI2: REVENUE GROWTH (PREVIOUS 3 YEARS)**
  This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.
- **GI3: GROWTH PIPELINE™**
  This is an evaluation of the strength and leverage of a company's growth pipeline™ system to continuously capture, analyze, and prioritize its universe of growth opportunities.
- **GI4: VISION AND STRATEGY**
  This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?
- **GI5: SALES AND MARKETING**
  This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

HORIZONTAL AXIS

Innovation Index (II) is a measure of a company's ability to develop products/services/solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets, and are aligned to customers' changing needs.

INNOVATION INDEX ELEMENTS

- **II1: INNOVATION SCALABILITY**
  This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.
- **II2: RESEARCH AND DEVELOPMENT**
  This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.
- **II3: PRODUCT PORTFOLIO**
  This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.
- **II4: MEGA TRENDS LEVERAGE**
  This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.
- **II5: CUSTOMER ALIGNMENT**
  This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, email permission@frost.com