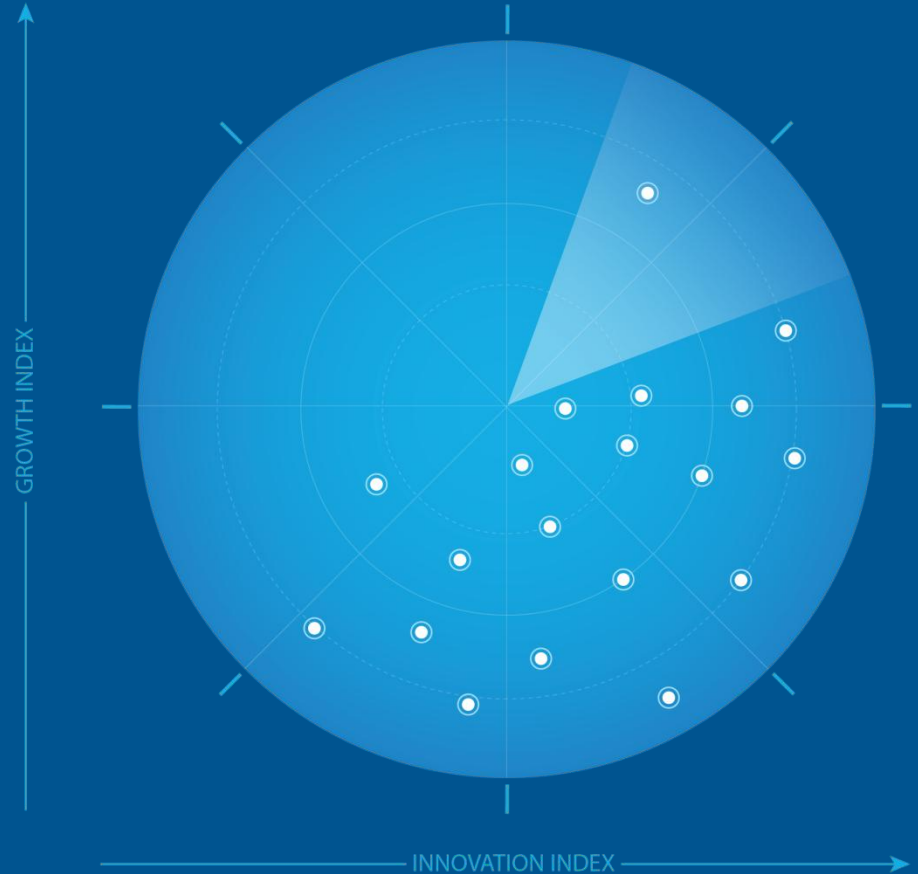


Frost Radar™: Cyber Threat Intelligence, 2024

Authored by: Martin Naydenov

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines



Strategic Imperative and Growth Environment



Strategic Imperative

Factors Creating Pressure on Growth

- The threat intelligence (TI) industry is growing steadily, fueled by low barriers to entry for start-ups due to venture capital injections, advancements in data scraping engines such as web crawlers, and the demand for proactive protection indirectly nudged by regulators and cyber-insurance firms. This has prompted nearly all cybersecurity vendors to offer some form of TI, ranging from basic telemetry data to comprehensive strategic threat reports. In response to this heightened demand and competition, more pure-play cyber threat intelligence (CTI) providers are integrating external attack surface management (EASM), and digital risk protection (DRP) capabilities, while cybersecurity platform providers are leveraging their economies of scale to enter the TI domain and get a piece of the pie.
- As TI capabilities become commoditized, vendors must invest in research and development (R&D) to expand their use cases, integrating more DRP, EASM, and generative artificial intelligence (AI) functionalities. The rise of AI presents both opportunities and challenges: while it empowers organizations to proactively enhance security, bridge talent gaps, and gain a strategic advantage in cybersecurity, it also enables threat actors to exploit vulnerabilities more efficiently.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- The integration of AI throughout the TI lifecycle enhances detection, response, productivity, and threat reporting, driving demand for AI-enabled TI solutions across industries and regions. This trend is expected to surge in the next 5 years, reshaping the TI landscape and compelling non-AI-enabled providers to adapt to these changes to avoid becoming obsolete.
- TI enhances security solutions by providing insights into emerging threats and attacker tactics, bolstering security ecosystems. However, practical implementation poses challenges, including quantifying TI's value and making compelling business cases. To navigate confusion and drive adoption effectively, vendors must focus on strategic marketing campaigns emphasizing outcomes and return on investment (ROI) rather than solely on capabilities.
- Geopolitical tensions and conflicts, such as the Russo-Ukrainian War, have a dual impact on the TI industry. On the one hand, it increases demand for TI because of heightened threats from nation-state-sponsored hackers. On the other hand, sanctions and mistrust constrain the industry, hindering partnerships and global expansion for cybersecurity providers. This geopolitical turbulence affects the cybersecurity industry, shaping demand for TI and influencing vendors' go-to-market (GTM) strategies, especially for vendors based in Russia and China that are operating in the West.

Growth Environment

- Advancements in AI, platform consolidation (such as the integration of external risk mitigation and management [ERMM] solutions), and the emphasis on proactive security measures will drive CTI industry revenue, with a compound annual growth rate of 33.5% projected from 2023 to 2028. On average, CTI participants included in this Frost Radar™ have seen revenue growth rates of 29% in the last 3 years, while marketing investments have averaged 17% of revenue.
- Acquisitions such as that of Mandiant by Google are accelerating the growth of the CTI industry. Cybersecurity platform providers from adjacent industries also are propelling growth by developing proprietary solutions or acquiring smaller CTI vendors. North America and EMEA will remain focal points for vendors because of the prevalence of large enterprises with advanced security maturity and substantial IT/cybersecurity budgets, but slightly higher growth rates in APAC and Latin America will reflect an upward trajectory in security maturity in these regions. Latin America and APAC also offer significant opportunities for Russian and Chinese vendors that face challenges expanding in North America and Western Europe.



Source: Frost & Sullivan

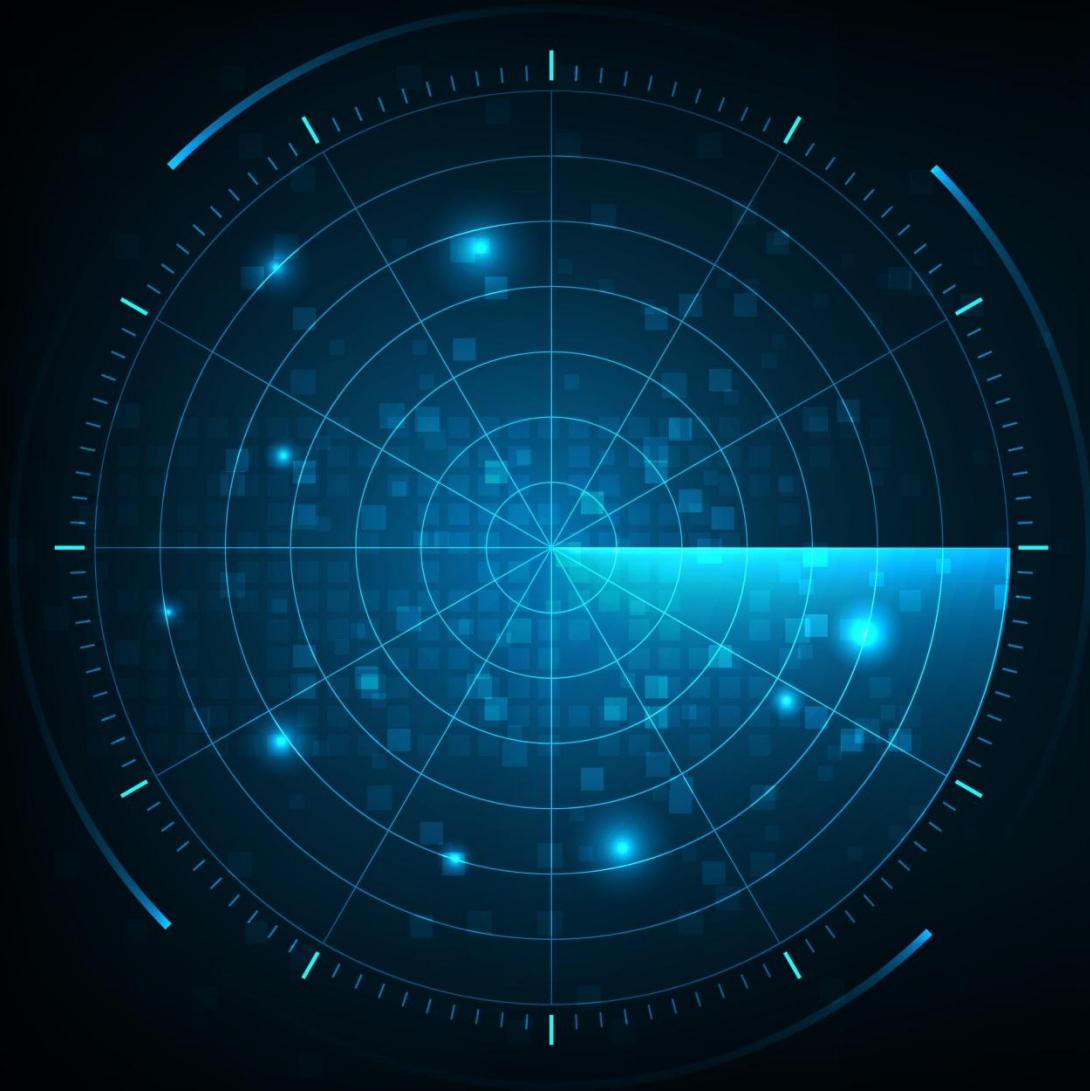
Growth Environment

- The technology, government, and financial verticals will continue to be the most profitable, with healthcare poised for significant expansion. This growth is driven by escalating threats from targeted phishing campaigns, supply chain attacks, and internet of things (IoT) vulnerabilities. Regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States also indirectly drive CTI adoption in healthcare, with organizations focusing on continuous risk assessments across their supply chains.
- CTI solutions are best suited for organizations with advanced security maturity, elevated risk profiles for phishing attacks, large IT budgets, and low risk tolerance—criteria typically associated with large and mid-market companies that have strategic risk management capabilities and requirements. As a result, Frost & Sullivan expects large and mid-market organizations to remain the most significant growth areas. Still, small and medium-sized businesses (SMBs) are increasingly targeted by threat actors and need CTI solutions. Through managed TI services and managed security service providers (MSSPs), CTI vendors can expand their growth pipeline and serve this traditionally underserved segment.



Source: Frost & Sullivan

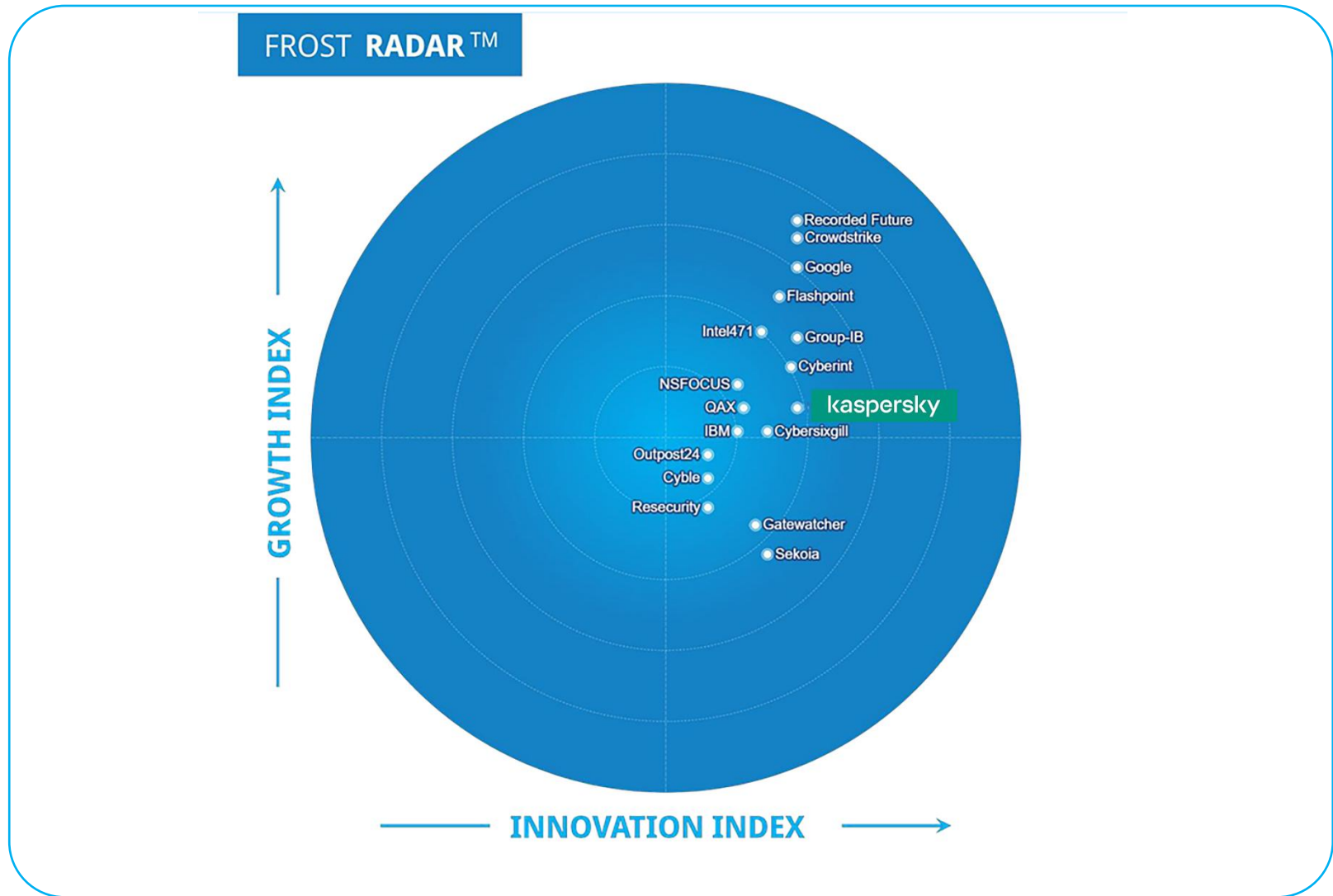
FROST & SULLIVAN



Frost Radar™

**Cyber Threat
Intelligence,
2024**

Frost Radar™: Cyber Threat Intelligence, 2024



Source: Frost & Sullivan

Frost Radar™

Competitive Environment

- The CTI industry has a wide variety of vendors with different profiles, value propositions, and use cases. On average, vendors invest 39% of their revenue in R&D. Recorded Future has the leading position on the Growth Index, holding a dominant global CTI revenue share with steady growth rates and strong execution of its vision. Recorded Future, Crowdstrike, Google, Group-IB, and Kaspersky lead on the Innovation Index because of comprehensive CTI capabilities, scalable innovations, high R&D investments, thought leadership in the CTI space, and robust innovation roadmaps.
- Notably, Kaspersky offers both CTI and TIP solutions, enabling them to ingest third-party commercial CTI feeds from other vendors.



Source: Frost & Sullivan

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

Company to Action: Kaspersky

Innovation

- Kaspersky's comprehensive cybersecurity suite encompasses a wide range of solutions including security information and event management, extended detection and response (XDR), managed detection and response, and network detection and response, underpinned by its TI offering. Its TI portfolio has 10 integrated modules spanning threat feeds and lookups to reporting and takedown services.
- Kaspersky is one of the few vendors that provide both CTI and TIP and can ingest third-party commercial data from other vendors. It has global customer support, and a research team spread across strategic locations to scale its solutions in a range of segments and provide highly contextualized threat intelligence services.
- With R&D investments between the 60th to 80th percentiles, Kaspersky has made numerous enhancements in recent years. In 2023, it introduced new threat lookup features, such as timeline analysis of IOCs and similarity lookups for malicious files, supported by one of the largest repositories with more than 25 years of historical data.

Source: Frost & Sullivan

Company to Action: Kaspersky

Innovation

- Kaspersky maintains a strong innovation roadmap and offers DRP and EASM use cases such as brand protection, social media monitoring, and asset management through its Digital Footprint Intelligence module. While it has yet to introduce generative AI capabilities to its customer base, they are on the roadmap for Q4 2024.

Source: Frost & Sullivan

Company to Action: Kaspersky

Growth

- Kaspersky has a global customer base with a market share between the 40th and 60th percentiles, primarily serving large and mid-market enterprises in the government, finance, and technology verticals.
- The vendor's extensive product portfolio presents numerous cross-selling and upselling opportunities. Its TI offering is highly customizable, with 5 pricing options and sets of capabilities tailored to the security maturity and budgets of various organizations.
- Most of Kaspersky's CTI revenue is generated through its distributor channel, achieving steady growth. However, its growth rates and marketing investments both rank in the 20th percentile.

Source: Frost & Sullivan

Company to Action: Kaspersky

Frost Perspective

- Kaspersky has an extensive product portfolio and comprehensive CTI capabilities, amplifying its innovation scalability. The vendor demonstrates a strong technology roadmap and is in the process of implementing generative AI capabilities, ensuring that it remains competitive with the other leading vendors.
- While Kaspersky has a global customer base, it is concentrated in Russia, Saudi Arabia, and the United Arab Emirates. Geopolitical conflicts and economic sanctions further restrict this Russia-based vendor's reach in North America and Western Europe. Kaspersky should expand its distribution channels and partner more with MSSPs to grow in Latin America and APAC and increase its marketing investments to the industry average and launch targeted campaigns in these regions.

Source: Frost & Sullivan



Key Takeaways

Key Takeaways

1

Cybersecurity vendors face significant challenges communicating their value propositions, especially for TI solutions. Many resort to fear-based marketing and gimmick capabilities, which lose effectiveness as organizations become desensitized to constant threats and dissatisfied with overpromises. Instead, vendors should highlight the unique benefits and positive ROI of their TI solutions. Vendors can present a more compelling business case as these solutions evolve into comprehensive ERMM and SecOps platforms.

2

Effective marketing campaigns should focus on tangible benefits, addressing pain points such as brand erosion, revenue loss, visibility constraints, and productivity limitations. Messaging must avoid overpromises and excessive buzzwords to prevent confusion. Implementing ROI metrics in product offerings, displayed in dashboards, is key to conveying value. For instance, CTI providers can showcase cost savings from identifying leaked credit card data, and TIP providers can highlight how eliminating redundant data reduces costs.

Source: Frost & Sullivan

Key Takeaways

3

Latin America, though the smallest TI market by revenue, holds substantial growth potential driven by economic, regulatory, and technological advancements. The region remains underserved, with Brazil and Ecuador experiencing high phishing attack rates. Frost & Sullivan found in a recent survey that 50% of Brazilian organizations use DRP and EASM solutions, with 35% planning to implement them in 2024. This indicates the growing adoption of advanced security measures, presenting promising opportunities for TI vendors. In Brazil, more than 50% of security products are acquired through resellers and more than 40% via direct channels.

4

While significant opportunities exist in North America, EMEA, and APAC, competition is fierce. Expanding into Latin America offers TI vendors a chance to establish a strong presence. Success in Latin America requires a well-balanced GTM strategy, including partnerships with local channels, customized pricing, regional offices, and local talent. Brazil, Mexico, Colombia, and Chile are particularly promising because of their large enterprises and unmet TI needs.

Source: Frost & Sullivan

Key Takeaways

5

Organizations struggle with visibility, limited resources, alert fatigue, and manual processes. AI technology complements TI solutions by enhancing security, visibility, and productivity. Full AI integration across TI ecosystems is ongoing, but current applications have already improved data analysis by providing historical context and identifying attack vectors. AI can also offer tailored reports, predictive risk analysis, workflow automation, and dynamic threat visualizations. To remain competitive, TI vendors must increase AI investment. Prioritizing R&D in AI empowers customers to fully leverage TI solutions. Partnering with AI providers to enhance and integrate AI capabilities is crucial, allowing vendors to address evolving customer challenges and boost growth prospects.

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, write to: permission@frost.com

© 2024 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan. No part of it may be circulated, quoted, copied, or otherwise reproduced without the written approval of Frost & Sullivan.