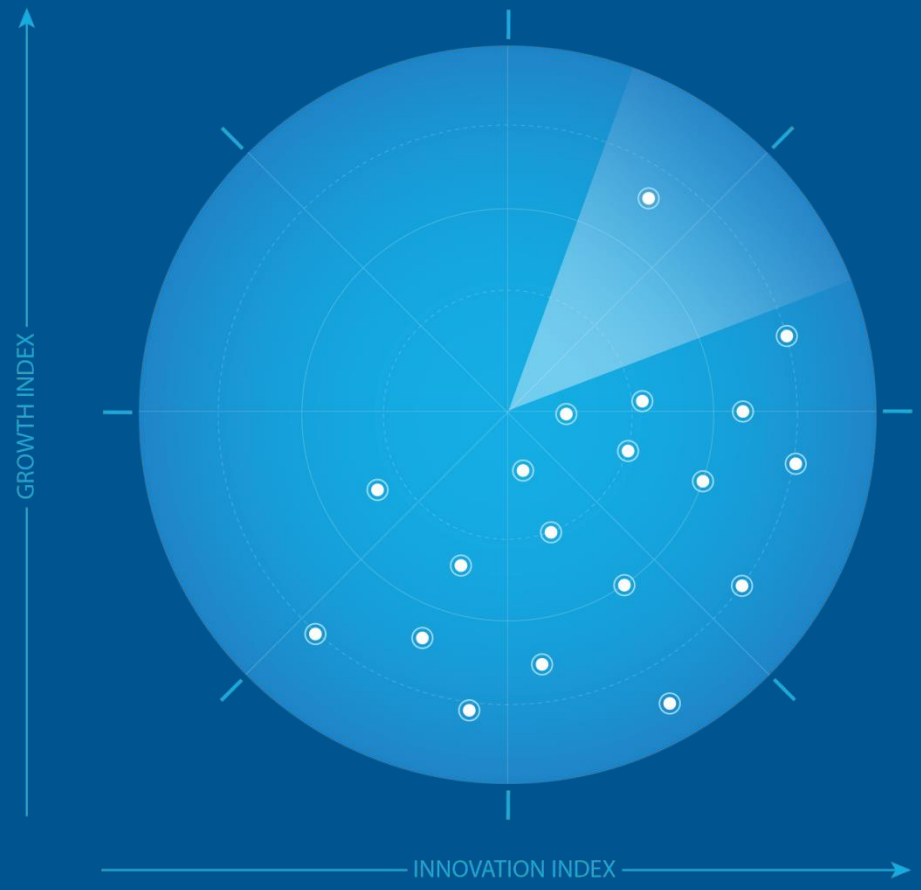
FROST & SULLIVAN

Frost Radar™: Managed Security Services in Europe, 2024

Authored by: Claudio Stahnke



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

June 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

Factors Creating Pressure on Growth

- The COVID-19 pandemic accelerated digital transformations and created a duality in the business world: enterprises have either embraced the shift to remote work that occurred at the pandemic's start or are pushing their employees once again to spend most of the workweek in the office. Talent that values flexibility considers whether a prospective employer offers a hybrid work environment or a work-from-home option.
- At the same time, the Russo-Ukrainian War and the Israel-Palestine conflict are causing disruptions and uncertainty throughout the region. State-sponsored cyberattacks are increasingly common and sophisticated. Value-chain attacks are particularly dangerous because they infiltrate the weakest links and spread rapidly across multiple areas.
- Comprehensive IT ecosystems that span on-premises and cloud workloads may generate hundreds of thousands of cybersecurity alerts daily and could overwhelm understaffed internal teams. Automation, machine learning (ML), and artificial intelligence (AI) capabilities are essential in these setups.
- A managed security service provider (MSSP) is often the best option to protect complex and fragile environments because it has the necessary expertise and workforce to mitigate cyber risks from a security operations center (SOC). It can offer vulnerability management, managed detection and response (MDR), breach and attack simulation, zero trust frameworks, and many other solutions and services to cover almost every imaginable use case.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Leading MSSPs have developed their own MDR platforms in recent years. These platforms need continued investment and development to stay ahead and compete with XDR- and MDR-focused vendors that can provide security solutions for more use cases. MSSPs retain an edge against XDR/MDR-focused vendors because of their wider portfolio and ability to serve a broader range of clients, including small and medium businesses that could find the price tag of XDR vendors too high. In upcoming years, MSSPs can use their broad portfolios to deliver additional capabilities on top of their XDR/MDR platforms and gain an edge over security vendors with fewer offerings.

- European MSSPs have an advantage in that they understand the complexities of European Union privacy and data regulations (including the General Data Protection Regulation, which limits the storage and manual or automatic processing of information essential for many security solutions) and regional differences in client demands. Enterprises in Northern Europe, for example, tend to have higher security maturity and more complex use cases. For enterprises in Southern Europe, providers generally must offer flexible pricing models, maximize the existing security stack, and guide companies along their maturity journey.

- As more vendors enter the MSS industry, the choices often overwhelm buyers. MSSPs must alleviate this confusion by showing the value that a broad portfolio supported by scalable managed security and consulting services can bring to companies of various sizes and security needs. Potential customers may need more education about MSSPs' value proposition and ability to offer customization for enterprises with unorthodox use cases.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Some MSSPs have one-size-fits-all packages, but top-tier firms can provide flexibility in payment models and strategic approaches, including quarterly meetings, documentation, and reports to emphasize the return on investment.
- Differentiators such as zero-trust architecture and integrations with IT, operational technology (OT), and the Internet of Things (IoT) are increasingly common. Their platforms will integrate with, and leverage managed XDR and MDR to provide much-needed synergy and scalability.

Source: Frost & Sullivan

Growth Environment

- European respondents to Frost & Sullivan's 2023 Voice of the Enterprise Security Customer survey revealed that security services constitute less than 10% of their spending. As enterprises try to streamline their cybersecurity portfolios and alleviate the workload on internal staff, Frost & Sullivan expects the budget allocation to increase.
- In Europe, cybersecurity budgets are growing slower than in the United States, with fewer than half of surveyed enterprises reporting budget increases. Interestingly, more than half of respondents stated that the Russo-Ukrainian War influenced their cybersecurity budget in 2023.
- Cybercrime continues to increase, with more sophisticated and frequent attacks each year. The impact of a security incident affecting critical infrastructure can be devastating for governments and enterprises alike. According to a 2023 report by IBM, the average data breach cost was $4.45 million, a 15.3% increase from 2020. Respondents to the Frost & Sullivan survey grossly underestimated the impact of a breach, with most respondents indicating an average cost of $1.7 million—roughly a third of the IBM figure.
- The increased competitiveness from pure-play MDR vendors, incident response companies, and similar security service providers that have carved market niches will compel MSSPs to accelerate the development of unifying platforms that integrate the security stack and work as a single-pane-of-glass management solution for all their services. This also reflects a push from the bottom as clients demand a simplified environment and easier-to-manage solutions that require fewer personnel and rely more on automation. Though MSSPs might lose some market share to these new competitors, revenue will continue to increase at a compound annual growth rate of 10% between 2020 and 2026 to reach $11 billion.

Source: Frost & Sullivan

Growth Environment (continued)

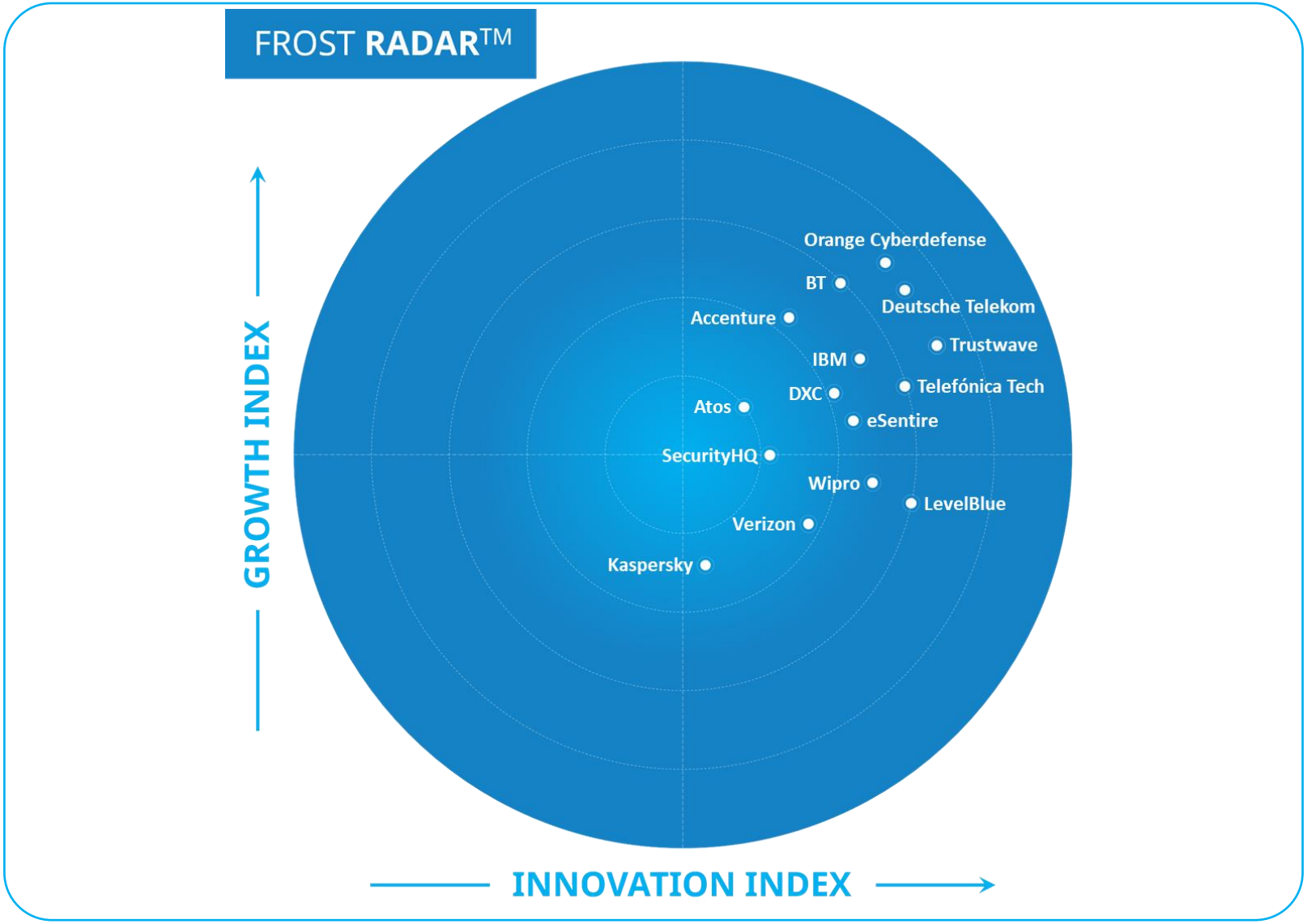
- Many specialization possibilities result in a heterogeneous market with distinct platforms and services. However, the megatrends are clear: keeping up with improvements in automation and ML-powered features, enhancing visibility over various environments, and providing additional third-party integration, extended coverage, and complementary security services that lessen the impact of labor shortages.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Managed Security Services in Europe, 2024

Frost Radar™: Managed Security Services in Europe, 2024



Source: Frost & Sullivan

Frost Radar™: Competitive Environment

- In a dynamic field that has experienced rapid growth, with more than 150 industry participants generating annual revenue exceeding $15 million in Europe, Frost & Sullivan has independently identified 15 leaders in growth and innovation through the Frost RadarTM analysis.
- Over the last few years, MSSPs have been at the forefront of innovation, improving available features and developing solutions that offer extensive visibility over the environment, advanced detection of the most pervasive threats, and all the knowledge and expertise of a veteran team of security analysts supported by AI, ML, and automation capabilities. This spirit of innovation has expanded security services to include virtual chief information security officers (CISOs), SOCs, and advanced threat intelligence that cater to clients' diverse needs. Every provider has its strengths and weaknesses; because of this, the market will continue to see an influx of new competitors—all with extensive coverage and portfolios—including telcos, consultancies, cloud providers, and system integrators, making this one of the most competitive spaces in the cybersecurity industry.
- At the high end of the market, solutions generally are comparable from a technical perspective, often checking the must-have boxes such as AI and zero trust. The true differentiation is in a provider's relationships with its customer base, beginning at the moment of first contact when potential clients are still evaluating the companies on their shortlist. At this moment, it is crucial to make them feel valued and integral to the industry's operations by understanding actual needs rather than trying to sell solutions that are easy to provide or more expensive but less effective for the use case.

Source: Frost & Sullivan

Frost Radar™: Competitive Environment (continued)

- Growth Index leader Orange Cyberdefense has built on top of successful acquisitions, expanding its footprint across Europe and relying less on France (its home market) to become a fully European player. Its focus on automation allows it to offer high efficiency and personalization to clients.
- BT remains the undisputed leader in the market, encompassing the United Kingdom and Ireland—one of Europe's most lucrative and mature. In recent years, it has expanded its offering with the notable launch of its Eagle Eye platform.
- Deutsche Telekom has a robust global presence and is the dominant player in the DACH region. It goes beyond using automation for simple anomaly detection; it uses AI to augment and optimize its human resources while addressing clients' concerns regarding the reliability of highly automated solutions.
- Trustwave is the Innovation Index leader thanks to its Trustwave Fusion security operations platform, which allows it to have vast visibility across the environment. Dozens of professional services augment Trustwave's value proposition.
- LevelBlue (formerly AT&T) is also an Innovation Index standout. It provides clients with a high level of flexibility thanks to a vast portfolio of MSS and professional services. At the same time, it offers adherence to strict compliance standards thanks to its expertise in working with government agencies.
- Telefónica Tech has simplified its offering since 2021, when it launched its unified brand, NextDefense, responding to clients' desire to consolidate their cybersecurity portfolios. This is notable, especially considering the acquisitions that have expanded Telefónica's capabilities in recent years.

Source: Frost & Sullivan

Frost Radar™: Competitive Environment (continued)

- Accenture is a leader in the space thanks to its dominant position in consulting and professional services, which provides it with a vast customer base for its MSS offering.
- IBM, one of the most prominent global players in the IT industry, can style itself as a one-stop shop, offering pre-sale consultation, post-sale support, and professional services. It has a strong presence in Europe, thanks to its brand and reputation, global clients with a European presence, and European players needing a global partner. IBM, though, still cannot provide the same level of local support as the native European players.
- Wipro allocates part of its R&D budget to support cybersecurity start-ups. This strategy is forward-looking because it represents a regular stream of new solutions that can be tested and implemented into Wipro's more comprehensive portfolio to keep it ahead of the competition.
- DXC has been making the onboarding process of new clients as smooth as possible, which can be a strong differentiator against providers with more standardized approaches. It also offers solid threat intelligence and adherence to regulations.
- eSentire's expertise in the MDR space strengthens its broader MSS offering. Its roadmap includes many promising features, most notably investments in Gen AI, which promises to give it a competitive edge.
- SecurityHQ invests roughly 40% of its revenue in R&D, which has allowed it to develop an interesting proposition centered on its SHQ Response platform, which has features ranging from analytics dashboards to asset management.

Source: Frost & Sullivan

Frost Radar™: Competitive Environment (continued)

- Atos, a more European player with an array of solutions at its disposal, recently had some financial troubles that have hindered its ability to sustain growth. Nonetheless, the French company remains a contender in the European MSS landscape.
- Kaspersky, a global player with its main headquarters in Moscow, has struggled recently because of geopolitical turmoil. Despite this, it has kept innovating in the MDR and MSS spaces, implementing services such as SOC consulting to bolster its value proposition.

Source: Frost & Sullivan

FROST & SULLIVAN

Companies to Action:

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

Company to Action: Trustwave

Innovation

- As one of the most innovative companies in the market, Trustwave provides a comprehensive suite of advanced MSS. The company integrates its portfolio through the cloud-native Trustwave Fusion security operations platform. This consolidation allows Trustwave to have unobstructed visibility across the environment and augment the capabilities of its entire stack thanks to synergy, providing increased resilience, flexibility, and accessibility for its customers.
- The most significant tools in the firm's portfolio are Trustwave's top-tier MDR service (delivering 24/7 MDR and proactive threat hunting that can be supported by digital forensics and incident response capabilities), co-managed SOC and co-managed SIEM services, supporting customers to deploy these technologies with the help and expertise of Trustwave's security advisors; managed SIEM for Microsoft Sentinel; advanced continual threat hunting; security technology management including NGFW, UTM, IPS, AV, WAF, email security, and more across on-premises or cloud environments; managed threat detection through the Trustwave Fusion platform; and more.
- Trustwave complements its offering with dozens of professional services and engagements that significantly contribute to its value proposition. These services can be categorized as security planning and strategy (such as various risk assessment services, security awareness, and incident response readiness); governance, risk, and compliance with region and industry-specific focus; policy and architecture assessment (such as security architecture consulting or an OT cyber program); testing and simulation exercises (including red/blue/purple teams and social engineering testing); and digital forensics and incident response. This combination of services enables Trustwave to close the loop, leveraging PSS to obtain essential information from the customer's ecosystem, vulnerabilities, and readiness to pinpoint its weaknesses and offer remediation with the provider's comprehensive MSS portfolio.

Source: Frost & Sullivan

Company to Action: Trustwave

Innovation (continued)

- Trustwave's Security Colony platform is another provider's innovative differentiator. The platform is loaded with a massive library of security resources developed for real clients, allowing customers to access Trustwave's IP and security advice for free. It includes compliance guidelines, a NIST CSF security maturity assessment tool, a vendor risk scoring tool, cyber awareness training strategies, and invaluable consulting advice for organizations across every industry vertical or maturity level.
- Trustwave invests significant resources in continuing the development of its portfolio. The firm is focusing on improving managed IoT/OT services (including expanded advisory services for these environments), extending its MDR and managed SIEM services with more AI/ML/automation features, continuing the integration of Trustwave portfolio, expanding cloud-native response actions and rulebooks, improving visibility and workflow of the Trustwave Fusion platform, and continuously enhancing its alignment to MITRE ATT&CK and D3FEND, among other innovations.

Source: Frost & Sullivan

Company to Action: Trustwave

Growth

- In January 2024, Trustwave was acquired by the MC² Security Fund, a private equity firm focused on growth advisory and investments in the security industry and an affiliate of the Chertoff Group. The acquisition and strategic partnership align with Trustwave's goals and will provide immense growth opportunities in the foreseeable future. The company continues to grow rapidly thanks to its solid strategy and comprehensive portfolio, which delivers flexibility to customers of all industries and sizes.
- Trustwave's strategy involves selling directly to enterprises and large businesses while supporting extensive channel partnerships that target the mid-market. Its security services and solutions are designed to help businesses on digital transformation journeys, supporting the company's strategy.
- The Trustwave Fusion platform makes it easy for customers to pick and choose which products to purchase, bundled, as add-ons to a service such as MDR, or separately, delivering flexibility in addressing their use cases. The company's customer focus also shines through the Security Colony platform, which dramatically increases value for the customer for free, helping many customers who might not get access to consulting engagements because of budgetary constraints.
- Trustwave leverages many different resources as part of its digital-first marketing strategy. These efforts include conducting vertical threat briefings, publishing SpiderLabs threat research, Trustwave blogs, and other proprietary content focused on specific industries, sponsoring in-person events, investing in social media and digital channels, and using more traditional approaches like account-based marketing. These resources increase brand awareness significantly and contribute to Trustwave's growth and expansion.

Source: Frost & Sullivan

Company to Action: Trustwave

Frost Perspective

- Trustwave understands the importance of collaboration in the cybersecurity industry. Security Colony is powered by the hacking ethos that programmers and developers in the free software movement have long since adopted, the idea that knowledge should be shared. Security Colony showcases many of the company's capabilities, including consulting and assessment services. It greatly benefits companies with tighter budgets for free and entices those with the resources to spare to partner with Trustwave. It provides untold value while creating numerous growth opportunities for Trustwave, and the company should continue to expand its features as much as possible.
- Trustwave's world-class portfolio shows the importance of leveraging professional services, assessments, and consulting to exalt and enhance managed services. The synergistic cycles these services promote are essential to better understanding customers' environments and delivering effective security outcomes. To maintain its competitive edge and retain its effective strategy, Trustwave should continue to invest in augmenting its existing products and developing new ones according to the most important megatrends, prioritizing OT/IoT security, visibility, integration, and AI.
- Trustwave should consider its generative AI and LLM strategy carefully; developing in-house, licensing, or acquiring can lead to different paths to success. These tools are important to several cybersecurity companies' offerings and will likely shape the landscape for the next three to five years.

Source: Frost & Sullivan

FROST & SULLIVAN

Key Takeaways

Strategic Insights

1

Frost & Sullivan's 2023 Voice of the Enterprise Security Customer survey, a reference point for this Frost Radar™, revealed a practical trend: a majority of respondents are adopting a combination of outsourced and in-house cybersecurity approaches—a choice driven by the reality that many enterprises lack the internal resources for a comprehensive in-house approach yet have reservations about complete reliance on external teams. This underscores the importance of flexible service providers offering solutions and services tailored to a client's specific needs.

2

Many executives consider expanding their internal cybersecurity teams to bring certain functions in-house and reduce reliance on external teams. However, establishing effective synergies between internal cybersecurity specialists and service providers' analysts can be complex, especially when the provider's analysts are not exclusively dedicated to a specific client—a situation often associated with higher-priced service tiers.

3

MSSPs should not just consider but deeply understand their clients' most effective approach to managed security. Organizations rarely fully outsource or keep all their cybersecurity in-house, often choosing a blend of the two. Best-in-class is not always needed; sometimes, "good enough" is the way to go, considering budgetary constraints and cybersecurity maturity levels. This client-centric approach is key to success in the industry.

Source: Frost & Sullivan

Strategic Insights

4

Organizations seeking to co-manage security with an MSSP partner need collaboration-oriented tools and guidance on their maturity journey. The MSSP's security team should be viewed as an extension of the internal one. The MSSP should be asked to provide information about turnover rates, as a higher rate will negatively impact the ongoing relationship between internal and external teams.

5

Conversely, MSSPs should be able to accommodate companies intending to outsource their security with broad, completely integrated portfolios. Periodic meetings, dashboards, and reports are essential to help clients understand the state of their security posture, risks, and challenges and allow the provider to demonstrate the ROI of dedicating money to cybersecurity.

6

Other ways for MSSPs to diversify themselves include:

- developing vertical-specific knowledge and portfolios;
- having a portfolio that is flexible and able to keep improving the security posture as a client's organization expands;
- devising pricing models and SLAs that are clear and easy to understand to avoid the risk of budgetary challenges if they are not fully understood; and
- being clear about data residency, especially in Europe, as clients might be wary of transferring their data outside the European Union in a region with different data privacy laws.

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 (BASE YEAR)**
  This is a comparison of a company's market share relative to its competitors in a given market space.
- **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