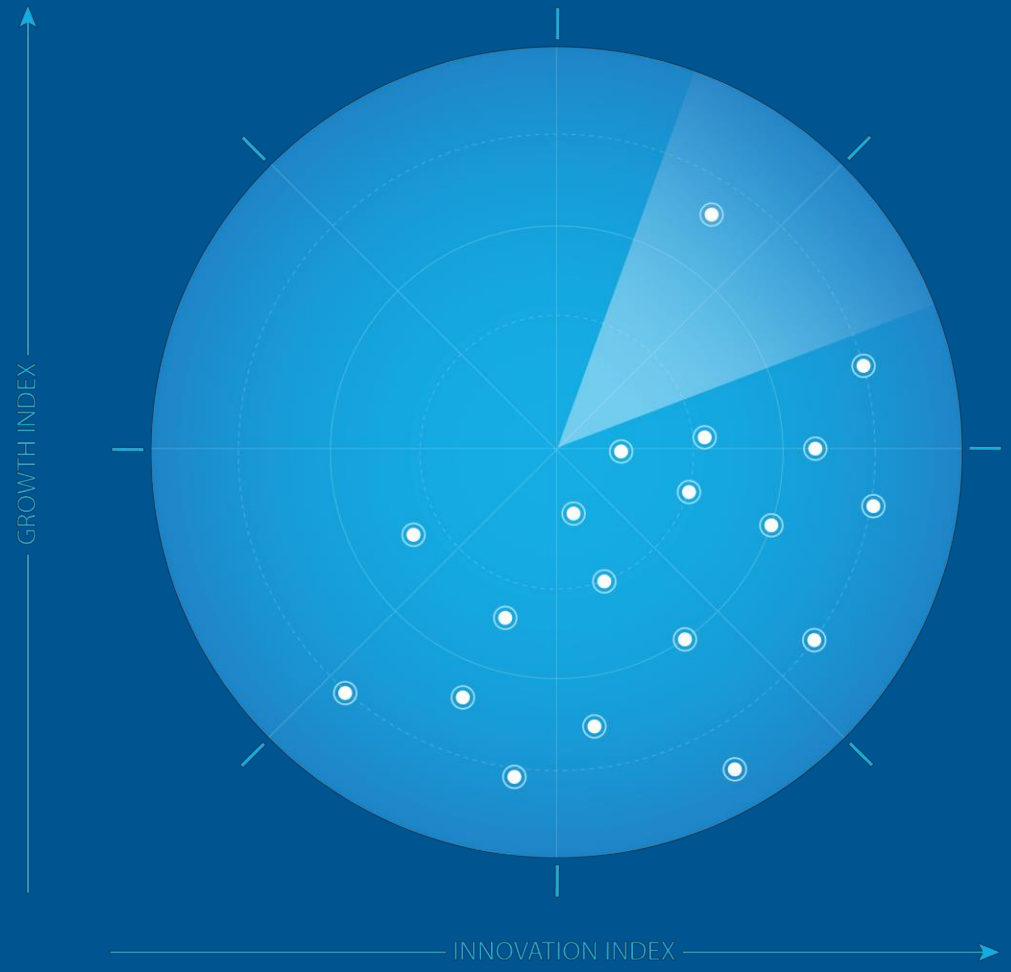
FROST & SULLIVAN

Frost Radar™: Americas Managed and Professional Security Services, 2023

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



Global Security Research Team at Frost & Sullivan

K7EC-74

February 2023

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

Every nation in the Americas has experienced significant social and economic turmoil during the COVID-19 pandemic. The economic setbacks resulting from this situation led to budgetary constraints and rethinking of priorities for enterprises of all sizes. The turmoil also forced many companies to adopt work-from-home models, with hybrid networks and more complex environments.

Even after the Americas fully recovers from the economic downturn, the consequences and changes to company culture and flexibility expectations will remain. Work-from-home as a standard forces enterprises to adopt hybrid cybersecurity models. At the same time, threats are more sophisticated than ever. Even a minimal security breach can lead to a security incident that compromises a company's entire value chain.

Protecting such environments requires increasingly complex solutions that are managed by skilled cybersecurity professionals. The best option that allows enterprises to focus on their business without neglecting security is a vendor that can provide and manage comprehensive cybersecurity solution ecosystems.

For a glossary of the cybersecurity-related terms used in this report, click here.

Source: Frost & Sullivan

Strategic Imperative (continued)

Over the past few years, managed security service providers (MSSPs) have improved the automation, machine learning (ML), and artificial intelligence (AI) capabilities of their solutions and services. Comprehensive ecosystems spanning on-premises and cloud workloads generate hundreds of thousands of alerts daily. It is challenging to handle cybersecurity needs without the aid of automation, but the reasoning and discerning capabilities of a skilled security professional are currently impossible for AI to match.

The acceleration of digital transformation, propelled by the push for automation and the lack of security personnel, has created the perfect market conditions for MSSPs to leverage. Leading MSSPs have been developing their own extended detection and response (XDR), managed XDR, or managed detection and response (MDR) services in the last three years. Continued investment and development will be needed to stay ahead in the market and compete with XDR and MDR-focused vendors that can provide security solutions for an increasing number of use cases.

In the next three years, MSSPs can take advantage of their wide portfolios to deliver additional capabilities on top of their MXDR/MDR services and gain an edge over security vendors with smaller offerings.

Source: Frost & Sullivan

Strategic Imperative (continued)

The MSS and PSS market is highly competitive and constantly changes to accommodate customer demands. The success of pure-play MDR, incident response, and other service companies puts further pressure on MSSPs.

Competitors in North America must serve the companies with the highest security maturity and most complex use cases that demand sophisticated security solutions. In Latin America, priorities include flexible pricing models, making the most of the existing security stack, and guiding companies along their maturity journey.

MSSPs need to deal with the challenges of buyer confusion due to conflicting marketing messages, the constant emergence of new solution categories, and the competition from adjacent spaces that claim to deliver on MSSPs' shortages. To show their value proposition and stand out against competitors, MSSPs will leverage their broad portfolios supported by scalable managed security and consulting services, as they are essential in securing any kind of environment belonging to companies of all sizes and security needs.

As differentiators such as zero trust architecture and integration with IT/IoT/OT environments become common, MSSPs will add these integrations to their security operations platforms. These will be platforms that deliver integration and leverage managed XDR and MDR to provide much-needed synergy and scalability to their offering.

Source: Frost & Sullivan

Growth Environment

The Americas managed and professional security services market continues to grow at a steady pace despite its maturity. Current market dynamics and drivers benefit MSSPs greatly and create the conditions for an 11.6% compound annual growth rate (CAGR) from 2022 to 2025, increasing from US$13.9 billion to US$19.3 billion, respectively. The Latin American market represents 10.5% of that total, but will grow faster, at a 17.5% CAGR.

The MSS segment is growing faster than PSS, but both will experience healthy revenue increases in the next three years. Professional services still account for the largest portion of the market and will continue to do so for the foreseeable future.

Thanks to the increased popularity that modern MDR pure-play companies are enjoying, MSS-focused providers have realized the importance of incident response, threat hunting, cyber-risk assessments, CISO as a service, and similar services. Leading MSSPs are introducing these services into their portfolios to build or improve customer relationships. At the same time, service platforms that integrate the entire security stack are a must for top MSSPs, and technologies such as managed XDR, managed SASE, and vulnerability management tools contribute to the growth of the managed security services space.

Source: Frost & Sullivan

Growth Environment (continued)

Large enterprises form one of the segments that contribute the most to MSS and PSS revenue, but small businesses and the mid-market are quickly adopting managed security in response to the increased amount and sophistication of threats. With the comprehensive portfolios and flexible pricing models offered by many MSSPs, companies with fewer employees are finding their security budgets are better spent outsourcing security.

The banking, financial services, and insurance (BFSI) industry contributes the largest portion of MSSP revenue. Other notable customer groups are government agencies concerned about the prevalence of critical infrastructure attacks and contracting with providers that can manage or co-manage their environments and increase their detection and response capabilities; and utility, construction, healthcare, and manufacturing companies that will benefit from OT and IoT security offerings.

Market revenue share is somewhat concentrated, with 53.6% held by the top 5 competitors. The top firms generate most of their income from large-scale managed security deals, customer engagements, and consulting deals with large enterprises and government organizations. As the PSS segment represents close to 63% of the market, organizations that focus on it will naturally dominate the space.

Frost & Sullivan study related to this independent analysis:

Growth Opportunities in the Americas Managed and Professional Security Services Market, K7ED (upcoming)

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™

Americas Managed and Professional Security Services, 2023


FROST & SULLIVAN
Companies to Action
Companies to Be Considered First for
Investment, Partnerships, or Benchmarking

Trustwave

INNOVATION

- **Trustwave is the Innovation Index leader** on the Frost Radar™. Its portfolio includes a world-class MDR service, co-managed SOC, managed SIEM, threat hunting, and consulting solutions such as penetration testing, enterprise penetration testing, cyber advisory, and incident response. The portfolio is integrated through the Trustwave Fusion security operations platform, augmenting detection and response capabilities of the entire Trustwave stack.
- Trustwave's Security Colony service is, in a word, revolutionary. It includes a massive library of security resources developed for real clients, as well as breach monitoring and ransomware readiness assessment.
- Trustwave's SpiderLabs team gives an edge to Trustwave in an increasingly competitive market, as teams of skilled cybersecurity professionals are the heart of any MSSP.

GROWTH

- **Trustwave is going through the most profitable period since the acquisition by Singtel six years ago**. It has a solid Growth Index score on the Frost Radar™.
- Trustwave's strategy involves selling directly to enterprises and large businesses while supporting extensive channel partnerships in charge of targeting the mid-market. Its security services and solutions are designed to help businesses on their digital transformation journeys, solidly supporting the company's strategy.
- The company's customer focus shines through in the development of services such as Security Colony that dramatically increase value for the customer and in the overall strategy of synergy between managed and consulting services.
- SpiderLabs continually authors thought leadership content, including recurring threat research and emerging threats, increasing brand awareness significantly.

FROST PERSPECTIVE

- Trustwave should continue expanding both its MSS and PSS offerings with new tools. Providing the right mix of managed and consulting services and the synergy between the two offerings will become more important as competing service providers (such as pure-play MDR vendors or incident response companies) try to take away market share from MSSPs.
- The development of Security Colony is underpinned by Trustwave's commitment to providing as much value as possible for its customers. The future for MSSPs lies in understanding that collaboration and consulting services should be exploited to augment MSS, and Trustwave should continue investing in these types of services.
- **Trustwave's focus on improving security maturity and providing cost-effective solutions to fit customer use cases** could be an asset for additional expansion.

Source: Frost & Sullivan

FROST & SULLIVAN

Strategic Insights

Strategic Insights

1

Security operations platforms, which integrate and augment managed security portfolios, serve as a way of **optimizing costs, increasing operational efficiency, and making analysts' lives easier**. Many **successful MSSPs already have security operation platforms in place** that provide a way to deliver services, integrate solutions, increase visibility, and provide a co-managed experience of the customer environment's security. MSSPs that do not offer a security platform yet **must invest in developing one** if they want to remain competitive in an increasingly fierce market.

2

Organizations in diverse industries such as manufacturing, healthcare, construction, and utilities **leverage OT and IoT** to enhance processes and augment critical infrastructure. The new generation of network security must account for these devices in addition to on-premises and multicloud infrastructure. To provide comprehensive protection across the entire customer environment, **MSSPs should invest in developing OT and IoT security, managed identity strategies, and managed SSE/SASE capabilities, which will help industrial customers develop a solid zero trust strategy.**

3

In the face of heightened internal and external competition, including pure-play MDR and MXDR, MSSPs should consider **pressing the advantage they already have by** further **expanding their broad scope.** Delivering complementary services such as incident response, cyber advisory, or CISO as a service as part of the regular MSS offering will **deepen the relationship with customers** and create **upselling opportunities.** MSSPs can compensate for their usually lower overall flexibility with much **higher scalability and lower costs from deploying economies of scale**.

Source: Frost & Sullivan

Next Steps: Leveraging the Frost Radar™ to Empower Key Stakeholders

Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Source: Frost & Sullivan


FROST & SULLIVAN
Frost Radar™
Analytics
85%

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.

Appendix

Commonly Used Cybersecurity Acronyms and Terms (1/2)

- **CISO** – Chief Information Security Officer
- **DDoS** – Distributed Denial of Service: An attack on a device or network that consists of flooding it with synthetically generated traffic, with the goal of making it unavailable to its intended users
- **DFIR** – Digital Forensics and Incident Response: A cybersecurity space focused on the investigation and remediation of cyberattacks
- **EDR** – Endpoint Detection and Response: An endpoint tool used to detect threats, contain the incident, and investigate with forensics and proactive hunting tools to provide immediate response and remediation
- **IAM** – Identity and Access Management: A set of tools that are used to manage and control user identity, permissions, and access
- **IoT** – Internet of Things: Physical objects and devices that can connect to the internet via technology
- **MDR** – Managed Detection and Response: A managed security service that provides a combination of security tools, controls, and human expertise to deliver proactive 24x7 monitoring of a security environment and perform detection and response
- **MSS** – Managed Security Services: Recurring or ongoing client engagements with contract lengths varying from 1 to 3 years; tend to include varying degrees of proactive monitoring of the customer's security environment and may include response services for cyber incidents
- **MSSP** – Managed Security Services Provider
- **NDR** – Network Detection and Response: A tool that monitors network traffic to detect and respond to threats; just like XDR and EDR, uses analytics, machine learning, and AI to boost its capabilities

Source: Frost & Sullivan

Commonly Used Cybersecurity Acronyms and Terms (2/2)

- **OT** – Operational Technology: Hardware or software used to control industrial equipment and processes
- **PSS** – Professional Security Services: Project-based client engagements with a defined scope, start, and end dates; typically include services such as risk assessment profiling, benchmarking, strategic security blueprint development, multiyear planning, and implementation services
- **SASE** – Secure Access Service Edge: A cloud-based solution that offers network and security services to protect users, applications, and data, regardless of location; includes SSE and SD-WAN (Software Defined Wide Area Network)
- **SIEM** – Security Information and Event Management: A solution that aggregates, consolidates, and analyzes data from different sources to provide useful information for detecting threats
- **SOC** – Security Operations Center: A team of multiple security analysts and experts that work together and deliver security services
- **SSE** – Security Service Edge: The security services subset of SASE, consisting of three integrated services — CASB (Cloud Access Security Broker), SWG (Secure Web Gateway), and Zero Trust Network Access (ZTNA)
- **XDR** – Extended Detection and Response: A solution category that consolidates and integrates other tools, providing visibility, analysis assisted by machine learning, and response capabilities across the environment; includes automation capabilities and can be offered as a managed service – MXDR

Source: Frost & Sullivan

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