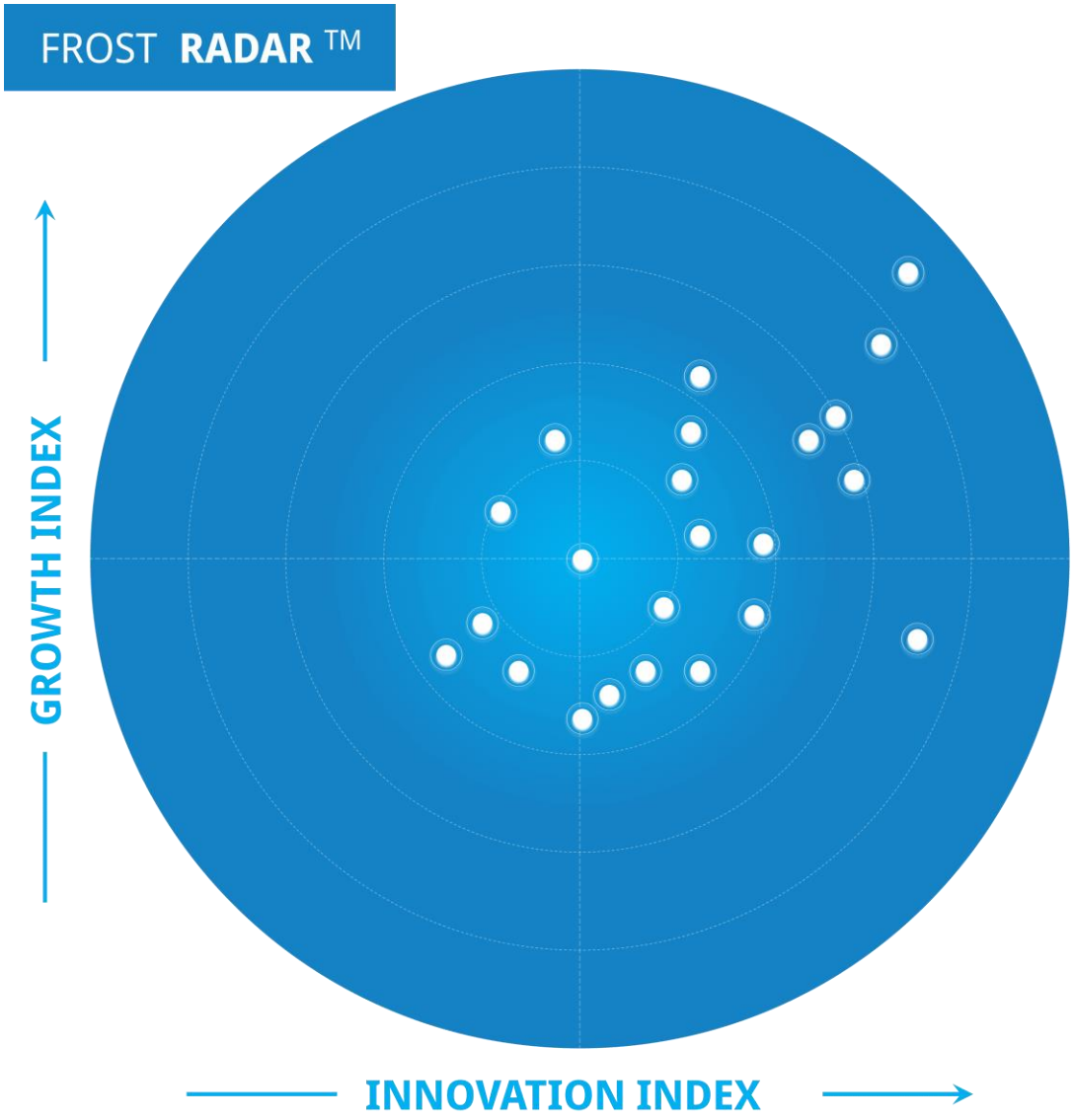
Frost Radar™

Managed Security Services in Europe, 2024

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

Authored by
Claudio Stahnke



MH14-74
June 2024

Research Summary

Managed security service providers (MSSPs) offer technology, expertise, and management for private and public sector customers, though the customer retains control and oversight. Standard services include distributed denial of service protection or mitigation, managed firewall, vulnerability management, and breach and attack simulation. Once provided onsite, these services are now primarily delivered through security operations centers. In the last two years, managed or extended detection and response have emerged as comprehensive service aggregators/security platforms that serve as single-pane-of-glass services through which providers deploy incident response and additional security capabilities.

Organizations decide to work with MSSPs primarily because of a shortage of personnel and expertise. MSSPs provide economies of scale that enable the organizations they serve to achieve significant savings by allowing the MSSP to manage, maintain, hire, train, and retain experienced cybersecurity professionals. Artificial intelligence, machine learning, automation, and collaborative features allow the solutions to work harmoniously with customer teams or fully manage their security stack.

Frost & Sullivan analyzes numerous companies in an industry. Those selected for further analysis based on their leadership or other distinctions are benchmarked across 10 Growth and Innovation criteria to reveal their position on the Frost Radar™. The publication presents competitive profiles of each company on the Frost Radar™, considering their strengths and the opportunities that best fit those strengths.

Strategic Imperative

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.

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. 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.

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.

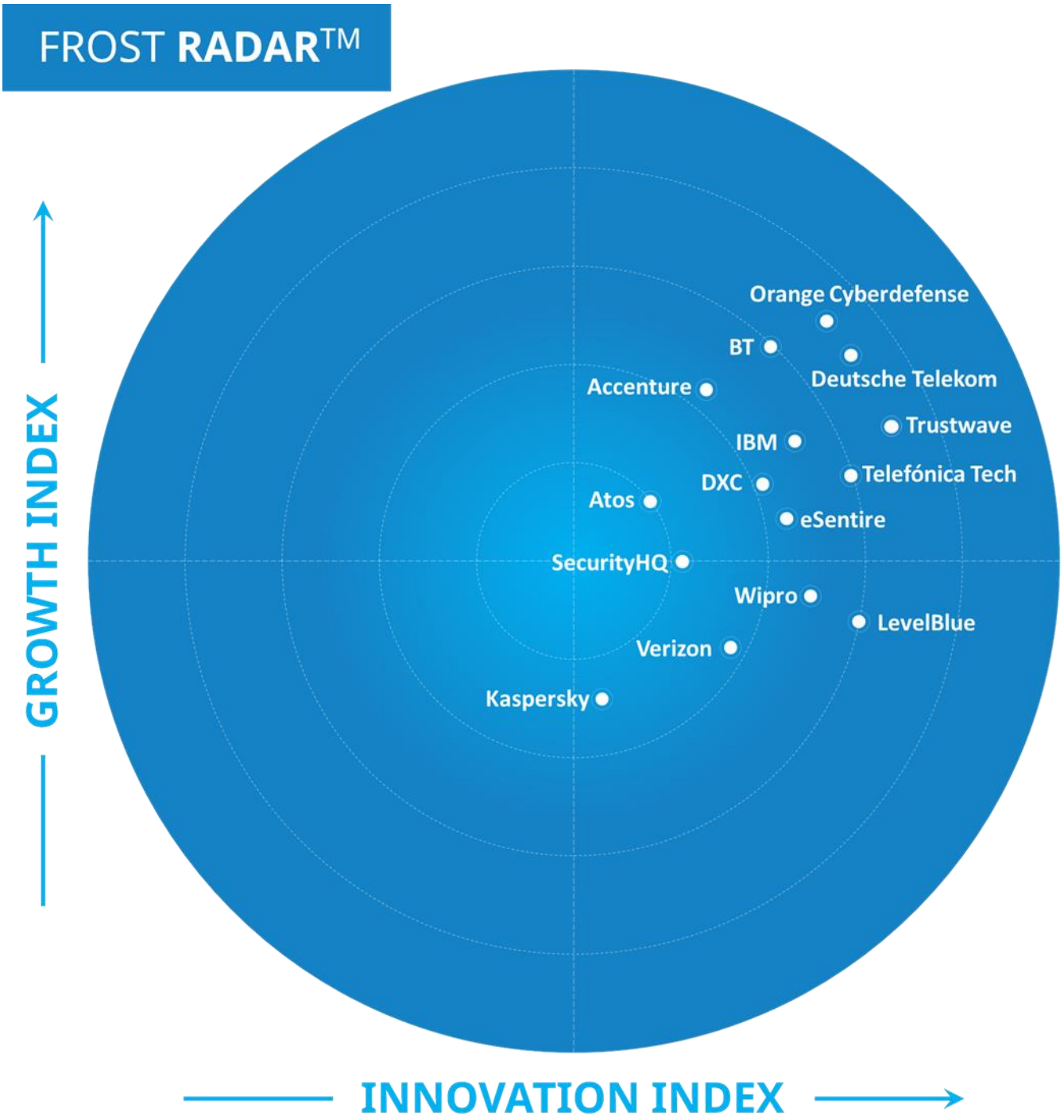
In Europe, cybersecurity budgets are growing slower than in the United States, with fewer than half of surveyed enterprises reporting budget increases. Interestingly, more than half of respondents stated that the Russo-Ukrainian War influenced their cybersecurity budget in 2023.

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.

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.

Frost Radar™



Source: Frost & Sullivan

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 Radar™ 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.

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.

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.

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.

Deutsche Telekom

Innovation

- Deutsche Telekom is a prominent player in telecommunications and cybersecurity, with a global presence spanning more than 50 countries and serving over 200 million mobile users and 25 million fixed-network lines, including a significant business segment in the United States through T-Mobile. The company has expanded its operations globally, focusing on Europe, Latin America, and Asia-Pacific. Its core focus lies in cyber threat detection and response, which is particularly underscored by its European facility's operations.
- Deutsche Telekom shifted towards a holistic security approach that considers security from an overarching perspective. This includes assessing the entire technology stack, processes, and business functions to identify vulnerabilities and mitigate risks effectively. It is planning to offer multi-source XDR telemetry as well as investigation, orchestration, and automation across its structure, which has been divided into five pillars:
  - endpoints
  - identities
  - connectivity (e.g., SASE)
  - cloud
  - OT
- Within these pillars, Deutsche Telekom has identified an ecosystem map that categorizes security tools into four types based on their integration and support within the MDR service:
  - Fully managed by Deutsche Telekom and integrated for deep analysis.
  - Tools with out-of-the-box alert ingestion, enrichment, and triage support integrated for deep analysis.
  - Tools using the vendor's API with out-of-the-box alert ingestion, enrichment, and triage support.
  - Tools used primarily for enrichment and implementing breach containment measures for rapid response.
- AI and ML play crucial roles in threat analysis, but Deutsche Telekom aims to go beyond continuous anomaly detection to decision augmentation and automation. This approach seeks to optimize human resources while improving response times and accuracy. There will be a gradual implementation and clear communication to address potential client concerns.

Growth

- Deutsche Telekom and its telecom operations, mainly in Eastern Europe and T-Systems, provide robust economic performance. This is evidenced by revenue exceeding €400 million from its security offering, derived from various sources, including infrastructure, network security, cyber defense, social services, identity and access management, and consulting services. These revenue streams underscore the company's diversified portfolio and strong market position.
- Looking at Deutsche Telekom's portfolio, the plan is to advance the Magenta Security Shield family with an MDR portfolio. Deutsche Telekom will shift from merely detecting threats to providing solutions for customers' security problems with different options for various target groups, offering MSS focusing on strategic market intelligence, cyber threat detection and response, and add-ons for professional services. Pricing and scalability will be simplified and made more efficient, too, as the aim is to onboard new clients within 30 days. Instrumental to this will be the customer portal, which serves as the primary interface, facilitating onboarding, incident reporting, documentation, and approval workflows. Plans include a mobile-friendly portal for enhanced accessibility and interaction.

Frost Perspective

- Deutsche Telekom caters to clients ranging from small and medium enterprises (SMEs) to large global enterprises across diverse verticals. Efforts to grow the SME segment are guided by leveraging sales channels, building trust, and offering tailored expertise to address their unique needs. While SMEs may not have the resources to implement complex security solutions, they still need robust protection against cyber threats. Recognizing these needs, Deutsche Telekom is developing tailored solutions and consulting services that are scalable and cost-effective. Challenges in this market segment, such as budget constraints and technological disparities, are addressed through strategic partnerships and customized solutions.
- Deutsche Telekom should expand its AI capabilities to offer standardized and highly automated solution packages. This will enable it to develop scale and offer a lower entry point to those SMEs with more constrained budgets or that do not yet consider cybersecurity a high priority.
- Deutsche Telekom’s future strategy entails enhancing its portfolio offerings, including managed security services covering enterprise, cloud, and OT infrastructures, focusing on IT and OT convergence. In addition, it should develop vertical-specific solutions and packages to outperform competitors, as different industries may have slightly different priorities regarding cybersecurity services and products.
- The company aims to simplify pricing structures and improve scalability to cater to a broader client base, from SME to enterprise. Future focus areas include market expansion and enhancing customer experience by integrating AI for improved service delivery. This push should also include the creation of highly flexible and customizable SLAs, as clients consider this a priority and will help create trust between customers and Deutsche Telekom.
- Recent initiatives include establishing real user groups within client networks to disseminate the latest threat intelligence, creating security business subsidiaries in select European countries, and strategic collaborations with partners to provide SOC services for vehicle security.

Strategic Insights

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

Legal Disclaimer