CyberDB
The Cyber Research Data Bank

R

CYBERSECURITY INDUSTRY REPORT

Are You Ready for The MSSP Revolution?

Elias Chachak and **Yoel Frischoff**

Cybersecurity Industry Report

Are You Ready for The MSSP Revolution?

October 12th, 2019

By:

Elias Chachak and **Yoel Frischoff**

Legal Disclaimer

Table of Contents

Authors

MSSPs – The Rising Stars of Cybersecurity Distribution

All over the world and across industries, organizations turn to MSSPs – Managed Security Service Providers. In this report, we analyze the reasons for that and suggest marketing/branding strategies for cybersecurity vendors and startups seeking to increase their traction through this emerging channel.

Cybercrime – A Major Challenge

Cybercrime is proving to be one of the biggest challenges facing humanity in the next two decades. Cyberattacks are the fastest growing crime globally, increasing in size, sophistication, and cost. Some predict that cybercrime damages will cost the world $6 trillion annually by 2021.

With 150 million ransomware attacks, plus a barrage of other cyberattacks, organizations and individuals are continuously exposed to both data and potential hardware damage.

According to a 2018 McAfee report, estimated cybercrime damages are soon expected to cost the world $600 billion, or 0.8% of global GDP, and is forecast to rise dramatically in the coming years.

In 2018, the average cost of cyberattacks was in the vicinity of $2 million per incident, and total spending on cybersecurity tools and services is growing strong, predicted to pass $248 billion by 2023.

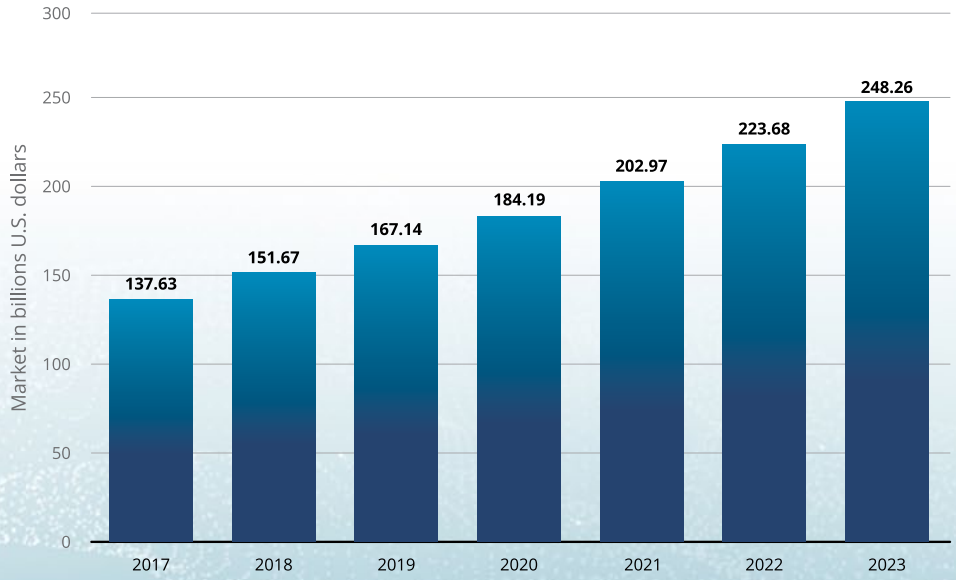


Figure 1 Cybersecurity solutions - Market size

Source: Statista.com

1. The Problem for Organizations

Chief Information Security Officers (CISOs), the executives responsible for organizations' cybersecurity strategy and implementation, are experiencing an increasing challenge.

The cyberattack problem has all but spiraled out of control. Processes and methods originally designed to tackle cybersecurity can no longer sustain the exponential growth in the number of cyberattacks, their severity and complexity, the increased number of attack surfaces, and the resources needed to tackle this barrage.

> Organizations struggle with exploding numbers of security incidents, and yet lack the magic bullet to stave those off.

1.1. Complexity of Cyber-Attacks

The threats we see are increasingly sophisticated, moving outside the realms of pure technology and firmly into the psychological layer. Cyber-criminals use our own behavior against us, as is evident from the rise of phishing and associated ransomware attacks—both types touch at the very heart of how much we trust established brands and how we respond to extortion.

Security risks to organizations are becoming increasingly complex with the addition of cloud, mobile, social media, Internet of Things (IoT), and big data technology.

1.1.1. Multi-Cloud Security

Organizations increasingly rely on multiple clouds that communicate and exchange data with each other. Separate security stacks within each cloud silo are no longer feasible; instead, organizations require transparent visibility and controls within each silo—as well as across all of them. Guidance for customers on data ownership, workload migration, and cloud federations are currently the domains of specialized companies.

An October 2018 Kaspersky Lab report revealed what CISOs consider to be today's top IT security risks. Cloud computing and uncontrolled cloud expansion by line-of-business applications (LOB); i.e. software designed to help businesses operate) topped the list.

Another survey found that 90% of cybersecurity professionals are concerned with cloud security. Specifically, when it comes to cloud computing, respondents cited three top security challenges:

- Protecting against data loss and leakage
- Threats to data privacy
- Breaches of confidentiality

1.1.2. Internet of Things (IoT)

IoT devices lack the processing power or memory to support anything but the most basic native security functionality—if at all.

These dumb devices present unique—and difficult—security challenges. It is still early days for IoT security, and the nature of innovations yet to come is hard to predict. One thing is certain, however: IoT will increasingly become a preferred attack vector for cyber-criminals.

1.1.3. Limitation of In-House SIEM / SOC

Another example is the global movement to add SIEM (Security Information and Event Management) to the security stack. SIEMs have proven to be a fundamental innovation for the aggregation of security data.

There is, however, a limit to the extent that organizations have been able to utilize SIEM technology for triaging true security events. Forensics involve several monotonous low-value tasks, which grow exponentially with each new alert, resulting in an increasing risk of human error.

Moreover, since digital interfaces are "on" 24/7, threats continuously pile up, requiring manual analysis and resulting in high levels of fatigue.

1.1.4. The Transformation of Security Operation Technologies

The outdated security operation center environment (SIEM/SOC) is facing a merging of tools in order to optimize the threat-hunting, investigation, and incident response challenges.

The following cybersecurity categories are being integrated in order to reach an operational and optimized platform:

- SIEM / UTM (Unified Threat Management)
- SOAR (Security Automation Orchestration and Response)
- Incident Response
- Case Management

- Security Analytics – including behavior analysis for users and entities
- Traffic Analysis and Recording
- Automated Threat Intelligence and Monitoring
- Knowledge Management

1.2. The Cybersecurity Skills Gap, a Talent Shortage, and Rising Costs

Manual forensics and hiring more staff are no longer viable options; there are simply too many events to control efficiently, with current systems requiring too many trained personnel to categorize and prioritize.

3.5 million security staffing shortages are forecasted by 2022 in the US alone. (CRN.com)

The current cybersecurity skills landscape is less than ideal. In McAfee's recent report about the security skills situation, "Hacking the Skills Shortage," they indicated that 83% of German and 75% of UK IT experts said there was a cybersecurity skills shortage.

Worldwide there are currently at least 1 million unfilled cybersecurity-related jobs. With cybersecurity salaries demanding at least 2.7 times the average of IT wages, recruiting a security specialist is both expensive and difficult.

According to recent studies, a cybersecurity talent gap exists across the US, where security staffing shortages are currently at around 747,000 (Momentum Cyber 2018 Almanac) and projected to hit 1.8 million by 2022 (Global Information Security Workforce Study).

Further, the cost of losing specialized staff has been calculated to average around 400% of their annual salary—adding to the spiraling cost expectation of personnel, given the high turnover rates for IT and cybersecurity personnel.

1.3. Solutions Pile-Up

The pressure of cyber threats has resulted in thousands of technology startups, most boasting a single-point solution. Information security officers rushed with matching demand, to the point of inefficiency:

> "The average enterprise is running 75 security tools in their environment. Meanwhile, all of these diverse toolsets create data and alerts without context of the environment as a whole". (Cybersecurity almanac 2019)

Organizations are overwhelmed with too many tools, few of which are integrated. These point solutions generate too many alerts for security teams to triage. Cybersecurity teams are struggling to integrate, operate, configure, or monitor the various tools that are part of their security infrastructure.

Strategies that may have functioned in the past to achieve incremental effectiveness of security initiatives now prove to be guaranteed to fail in the future.

1.4. Cost of Cybersecurity operation

The cost of hiring, retaining, and educating cyber professionals and teams in 24/7 shifts has proven to be very expensive, mainly for mid-size organizations lacking economies of scale. Retaining professionals after investing in training them proves to be a challenge as well. Losing security experts and subcontractors is a major hit to the security teams, and results in unexpected additional security budget costs.

2. Migrating To MSSP: Benefits for the CISO

The burden of cybersecurity needs to be somehow met with proper measures—hence the advent of the Managed Security Service Provider (MSSP).

MSSPs do not restrict themselves to catering to SMEs. Large corporations augment their own SOC operations by regularly employing MSSPs as a backup to their operations. They use MSSPs to manage SOC operations during non-working hours or to test newly added technologies within an isolated sandbox.

Most MSSPs base their infrastructure on cutting-edge technology, accumulated know-how, and robust operations. These building blocks offer the benefits of automated processes, centralized control, and economies of scale.

MSSPs employ their teams to simultaneously monitor the security posture for hundreds of clients. Through automation and knowledge accumulation, they can keep up-to-date versions of the myriad tools required for their customers, as well as a map of concurrent threats, thus optimizing response method and uptime.

2.1. Key Benefits

- Fully Autonomous Platform: addresses the widening skill gap, reduces fatigue, & improves ROI
- Faster Problem Triage: reduction in Mean-Time-To-Resolution (MTTR) and Alert Volume
- Advanced Correlation and Analysis across multiple customer sources
- Full Enterprise Visibility: identifies and mitigates advanced threats missed by single (siloed) tools
- Advanced UEBA (User and Entity Behavior Analytics) and Forensics Capabilities
- Automated Data Enrichment and Contextualization
- AI and Machine Learning: advanced organizations will figure out how to incorporate artificial intelligence or machine learning into the incident response process
- Today's enterprises will continue to struggle to manage their siloed tools and overstretched personnel; they are expected to increasingly gravitate towards MSSPs.

2.2. Economies of Scale: Specialization and Optimization

Using trusted MSSPs, organizations are protected against personnel cost, loss, recruitment, and retraining, and are assured, through SLAs, of an agreed upon/acceptable level of service.

Further, CISOs will see an operational advantage, as they can source all or part of their technology stack from a single point of contact, relieving management overheads.

2.3. The Evolution of MSSPs

MSSPs evolved to offer an attractive, ready-made alternative to an enterprise building its own in-house team of cybersecurity experts. This, coupled with the use of advanced technologies, helped bolster enterprise cybersecurity posture, improving outcomes, and managing for the spiraling costs of keeping a firm secure.

MSSPs have evolved in various ways;

- Some traditional service providers—taking notice of the ever-increasing demand for internet security—have added managed security to their portfolios. Examples include some incumbent telecom operators, such as Telefonica, Orange, and AT&T.
- Other traditional channel partners, such as value-added resellers (VAR) or consulting practices, are adding Managed Security Services as an additional security offering or as a spin-off (See Deloitte and CapGemini).
- Still other MSSPs have come into existence as brand-new entities focused solely on cybersecurity offerings, such as SecureWorks (global MSSP) or Excellium (local MSSP).

Some industry observers have asserted that every channel company is a "security provider" to some extent, as nearly every aspect of a client organization's operations features some cybersecurity components.

MSSPs have long targeted large enterprises, but as security threats evolve many are now focusing on providing managed security offerings to the small- and medium-sized business (SMB) market as well.

2.4. MSSP And MDR

Gartner defined the cyber category of MDR (Managed Detection and Response) services that allow organizations to add 24/7 dedicated threat monitoring, detection, and response capabilities via a turnkey approach *(Market Guide for Managed Detection and Response Services)*.

The MDR capabilities allow MSSPs to extend their services and use behavior analytics of the network traffic to detect attacks in the organization's network. In this case, MSSPs make use of EDR (Endpoint Detection and Response) products and threat-hunting services.

The services of MDR providers leverage technologies at the endpoint and within network layers that generate and collect security events and contextual data, supporting both the detection of threats and incident investigation, such as forensic data.

Additionally, there is a focus on threat analytic detection techniques, threat intelligence, and incident response activities.

2.5. MSSP Taxonomy

- **Pure Plays**: smaller, privately held, MSSPs that are completely focused on security services, with SecureWorks as a leading example.
- **Network and telecom operators**, offering managed services and tools such as firewalls, WAFs, IDS and other network-based security technologies. Examples: Telefonica, Orange, and Verizon.
- **VARs and IT system integrators**, either local or global, such as CapGemini and Atos.
- **Security consulting** providers, such as Deloitte and E&Y.
- **Some product vendors** (mainly endpoint detection vendors), such as CrowdStrike and F-Secure, offer managed services mostly based on the use of their own product.

3. A Changing Cybersecurity Value Chain: Towards Consolidation

The emergence of MSSPs heralds a new era for the cybersecurity market, changing the competitive landscape from fragmentation to consolidation. This has been long in the making, as is typical with technology markets evolving, cybersecurity included.

Historically, consider the development of the domain in a 3-phase process:

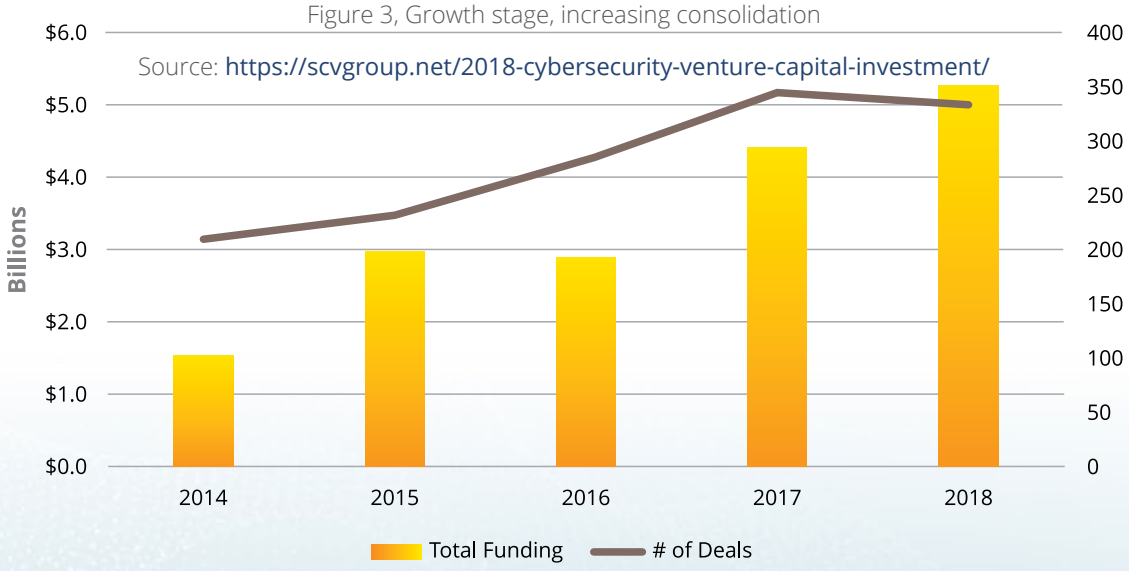
1. Discovery: exposure of cyberthreats.
2. Initial Response: myriad companies scramble to provide solutions to the newly discovered threats and scenarios; regulators follow suit, enforcing rules and standards.
3. Consolidation: Users start sourcing solutions from increasingly concentrated integrators, who can offer a one-stop-shop approach, reducing clutter and picking winners from losers on behalf of CISOs.

The Cyber security market is maturing. Consolidation is the next step.

Global Cybersecurity VC Investment

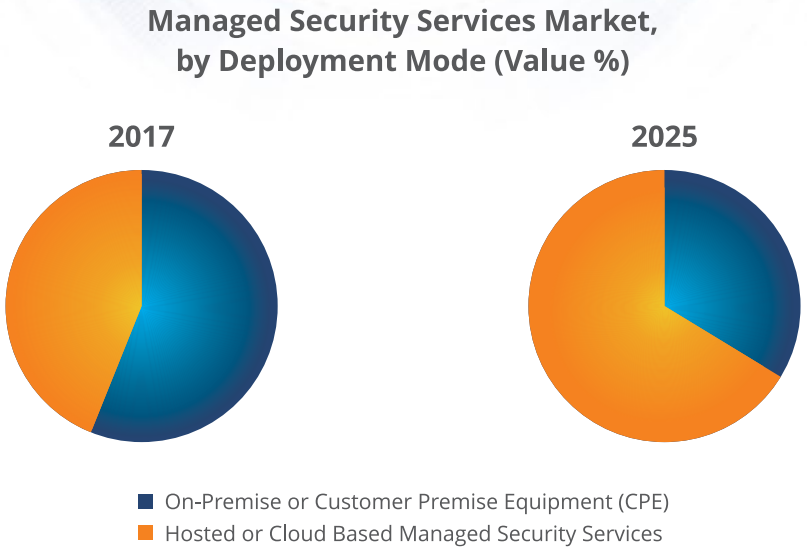
Figure 3, Growth stage, increasing consolidation

Source: https://scvgroup.net/2018-cybersecurity-venture-capital-investment/



4. The Growth of the MSSP Market

The demand for cybersecurity services is only expected to grow, according to several market research reports. Research firm MarketsAndMarkets, for example, forecasts the security services market will reach about $34 billion by 2021. This figure corresponds to 25% of total global cybersecurity spending (products and services).



Currently, around 50% of firms are turning to an MSSP to help them develop and implement their internal security strategies. This is expected to grow, with Gartner predicting that 83% of all companies have plans in place to outsource IT security in the next 3 years. This is creating a large market for MSSPs, which is expected to be worth $33.68 billion by 2021.

Where vendors once had to go to individual CISOs, pitching the value of their products, they now have MSSP CTOs as their audience. This makes sense, since there are a thousand times more individual customers than integrators. It is more efficient to vendors to concentrate their attention on the relatively few MSSPs.

5. How Do MSSP CTOs Choose Their Technology Stack?

Based on our discussions with the management of a number of local midsize MSSPs in Europe and the Americas:

- **How many point solutions do you integrate?**

  An MSSP typically implements 5 to 15 third-party security solutions as a means to optimize its day-to-day operation. Some of these solutions are also being resold or integrated at the customer site (not as a part of the MSSP operation).

- **How do you keep threats knowledge up to date?**

  Partnering with at least 10 suppliers of threat intelligence sources. Darkweb as a source is a must.

- **What parts of the service do you build in-house?**

  60% of MSSPs have developed one or more security operation solutions in-house. Examples are SIEM, threat intelligence, reporting, dashboard, and risk posture.

- **What are your criteria for selecting point solutions?**
  - Satisfying the criteria of the product
  - Maturity of the product
  - Technical support
  - Viability of the vendor
  - Vendor's openness for partnership

6. Going with the MSSP - Practicalities to Consider

6.1. From a Stand-Alone Product to a Service-Driven Component

Functional integration and orchestration come into focus as MSSPs integrate dozens of point solutions into a single environment to a centralized SOC. Eventually an MSSP integrated platform will feature its own dashboard and management consoles.

To be integrated within MSSP stack, products can no longer remain purely stand-alone solutions. They must be able to integrate into that unified management hub with its assorted set of dashboards, co-existing with other products and functionalities.

Such integration entails the disconnection of individual functionality from user interface; now each function in the technology stack will be displayed, monitored, and controlled via a unified console/dashboard software—whether in a single or multiple view.

It also requires each point-solution provider to "play nice," co-existing with an ever-changing array of solutions and communicating in a standardized protocol.

Using generally accepted terminology and adhering to machine-human interface best practices, vendors will be required to ensure that MSSP personnel get critical information in a timely manner, allowing proper action to be taken.

6.2. Business Model Transition, Go-To-Market Transition

As they grow, asserts CrossBeam Blog, vendors turn to channel partners for two main reasons:

1. No one company can expect to control a customer's entire technology stack
2. No one company can realistically reach all its potential customers

Whereas direct-to-customer vendors work directly with CISOs and their teams, MSSPs bundle several point solutions over a shared backbone to offer their customers an external comprehensive security stack, which they typically market as a subscription service.

MSSPs tend to work with hundreds of customers, often thousands. Scale is, therefore, the main advantage for vendors approaching them. This requires the right mindset in terms of a business model.

The emergence of MSSPs represent a major change in go to market for security vendors.

The York Group found that for SaaS software vendors selling in the US, the discounts offered to partners tend to stabilize on 50% of first-year revenue, and 30% for consecutive renewals.

ROW sales typically see 10% **higher** discounts on both parts, to compensate for smaller markets and higher operational costs.

Such discounts are offered when the channel partners engage in pre-sale, marketing, promotional, and support activities—and the MSSP model supports this delegation of tasks, which should accelerate growth—leaning on the scale and reach of MSSPs.

The transition in the go-to-market is as radical as is the change in business-model, since revenue, cost structure, and resulting contribution margins are expected to be different. At the same time, successful partnering should accelerate growth, bringing in economies of scale coupled with market dominance.

6.3. Shifting Channels - A Potential Conflict

There is, however, one inherent conflict in the transition from direct-to-customer to MSSP partnering, especially for vendors who have already gained a track record but are now compelled to adapt to an environment dominated by MSSPs: wherever they built and maintained an independent brand, working to increase awareness, they now need to turn to white-labeling under an MSSP umbrella, forgoing potential lateral growth.

Vendors transitioning from stand-alone products to point solutions integrated within a larger technology stack must carefully consider how to maintain their independent identity, and at the same time build the brand needed to penetrate the MSSP segment—operating more as an OEM.

Well-known vendors may encourage MSSPs to operate as channel partners, offering the vendor's solution to their respective customers without concealing it through white-labeling. An interim period may require management of both direct and MSSP channels—possibly maintaining different sub-brands catering to these specific audiences.

6.4. Courting MSSPs

Mapping relevant MSSPs is not an easy task and can be very tedious, especially if we are looking for mid-size, specialized and/or industry sector focused MSSPs. This is mainly because in many cases, Managed Security Service is a subset within the activities of the cyber-consultant practice or the system integrator's business.

Except for some worldwide global MSSPs, most MSSPs act locally for reasons of expediency (proximity to the customer) and data privacy regulations. Relevant MSSPs should be mapped by country and sometimes by region within a large country.

Once you identify your MSSP(s) of choice, make sure you understand their offering and their needs:

- Do you need to work with a global or mid-size MSSP?
- Is it focused on specific industry sectors?
- How does the MSSP source and integrate third-party solutions?
- How does it treat partners?
- Does your solution bring additional value to your target MSSP?
- How compatible is your technology to their backbone?
- Is your product architecture ready to be used by MSSP?
- Do you have a sustainable, hard-to-copy advantage?
- Do your KPIs match those of the MSSP?

7. Who are the Natural Partners for MSSPs?

CYBER CATEGORY	DESCRIPTION
SOAR vendors	Orchestration of incident response Automation and Orchestration tools augment threat prioritization, capability amplification, labor reduction, and consistent workflow
SIEM	Security Information and Event Management for managing the security logs
Threat hunting	Machine learning for quickly identifying the threat
Forensics	Investigation suite for understanding incidents
Threat Intelligence	Tools to crawl into the open web and the darkweb to find suspicious threats and blacklisted URLs and IP addresses
Breach simulation	Automatic Penetration Testing to identify breaches in the organization • Vital for security infrastructures that are constantly changing, and used to identify ill-advised or poorly planned changes • More efficient than manual regression testing, and an easily repeatable process
EDR	Endpoint Detection and Response
DDOS and Web Protection	Distributed Denial of Service protection and Web Application Firewalls (WAF)
Risk Posture	Security risk monitoring and presentation, providing a 360-degree picture of the Threat Landscape, to effectively protect the environments from malicious intrusions, and to detect and mitigate them when they do occur.
Anti-Phishing	Phishing attack simulation and awareness against phishing attacks

CYBER CATEGORY	DESCRIPTION
Network Security	Firewalls, Next Generation firewalls, Software-Defined Perimeter tools
Machine Learning	• Accelerates the decision-making process for prevention, detection, and response • Recognizes patterns and outliers that humans cannot efficiently analyze • ML solutions operate best at scale
Platform consolidation	• Consolidating the functionality of the security infrastructure into a single platform • Working with expert solution architects to help organizations ensure they are maximizing the efficiencies of these integrated platforms

8. Adapting the Product to MSSP Integration Needs

The operation mode of MSSPs has led them to form partnerships with hundreds of cyber-security vendors, in a combination of two models:

- Integrating vendor technology into their own stack, optimizing their solution, or
- Reselling vendor products to their customers.

The increasing role MSSPs play in managing cybersecurity and response for enterprises has led vendors to regard them as a major, customer-facing, channel partner. Vendors are:

- adapting their go-to-market strategies towards using MSSPs, both as a major sales channel and as a validation for their solutions and concepts.
- adapting their products to MSSP needs, increasingly developing multi-tenant, white-label products; MSSPs can deploy their solution portfolio for their customers, and they can still provide central orchestration and management.
- setting up managed services for their own products, as second- and third-level support for MSSPs offering their services.
- adjusting their training programs for MSSPs, including independent and full operation of the product and services by operators and analysts. Advanced training will need to be developed to cater to experienced MSSP operators.
- using MSSPs as design partners, for validation and for fine-tuning their offering to the highly skilled MSSP operators.
- Adjusting pricing strategies to fit MSSPs pricing policies.
- Large MSSPs have developed their own management and monitoring solutions, expecting cybersecurity vendors' products to be easily integrated and onboarded. Vendors need to offer MSSPs APIs to manage their products without the need for silo management screening.
- Increasing RESTfulness among market-leading security companies, creating a new opportunity to integrate multiple security technologies through new Managed Security Services offerings.

9. Marketing Consequences

In the pre-MSSP era, cybersecurity vendors needed to allocate their marketing efforts over different sectors, spreading thin over industries from the financial sector to pharma, retail, public, and government. Similarly, an endless search for local channel partners was needed to provide sufficient coverage in key markets, stifling growth.

The advent of MSSPs affects the go-to-market approach cybersecurity vendors employ. They can now shift their marketing efforts to concentrate on these strategic partnerships—narrowing their scope to a few dozen strategic partners, who will in turn reach out to the larger mass of end customers.

Scaling up via partnering requires vendors to change their value proposition, consequently alter their messaging, as well as their choice of media channels.

9.1. Promotion Strategies

A change in targeting brings change in promotion venues and efforts. Strategies such as account-based marketing make more sense in this context, where geography-based sales executives will nurture a focused set of accounts, augmented by a few global account managers, catering to the mammoths of the industry.

Industry events, for instance, will be efficient venues for relationship-nurturing efforts, with manageable numbers of high-value leads.

9.2. Exposure

In this new environment, specialization is key. As vendors are targeting those high-value, highly knowledgeable leads, they need to stand out and be highly visible.

All media channels are in play:

- Company web sites
- Solution landing pages
- Social media
- Blogs and dedicated media
- Industry events
- Content strategy and thought leadership
- Analysts, influencers, and investor relationships

9.3. Key Messaging - Addressing MSSPs

Messaging and content marketing will now also change scope to address pains of MSSP CTOs, in addition to the pains of CISOs.

The core values that will dominate the discourse:

- **Product Market Fit**: Vendors need to find and communicate a clear and actionable problem-solution set, including owners and differentiators.
- **Value**: Vendors need to demonstrate a credible ROI calculation; a challenge in the cybersecurity market, behaving similarly to insurance, making it difficult to quantify.
- **Competitive Advantage**: Vendors need to carefully articulate how their positioning builds on their comparative strengths over the competition.
- **Credibility**: This can be achieved by emphasizing investors, partners, customers, and design partners, awards, and IP.
- **Synergies**: Vendors should emphasize how their product can fit into the roadmap of the MSSP partner. How their competitiveness and business can be increased through the relationship.
- **Responsiveness**: In order to mitigate culture differences between small vendors and large integrators, including the geographic distance with partners.
- **Reliability**: With each solution a single point of failure, MSSPs will pick tried-and-true solutions first.
- **Team play**: No prima donnas allowed on board. Each distinct component must "behave" in terms of collaboration, load, and attention required.

10. Challenges and Opportunities

In this analysis, we have shown that the imminent dominance of the MSSP channel in the cybersecurity market will force vendors to adapt.

Through the interim period forecast until 2025, cybersecurity startups must navigate a mixed channel market: They will first have to address individual target organizations, appealing to their CISOs, to gain initial traction and credibility. Then they will have to reveal to MSSP CTOs the virtues of their solution(s), such as their scalability readiness, their innovativeness, and the way they allow MSSPs to manage profitably.

The opportunity is big, as some MSSPs have the potential to catapult a vendor's sales by two orders of magnitude, on a single sale.

Authors:

Elias Chachak, CyberDB

Over the past several years, CyberDB (www.cyberdb.co) has aided cybersecurity vendors in (re)shaping their product strategy to reach Product Market Fit—specifically targeting MSSPs.

CyberDB's close relationship with MSSPs worldwide helps them evaluate and scout for new technologies and solutions.

CyberDB's online knowledgebase covers over 5,000 cybersecurity vendors, sales, and integration channels worldwide.

Contact me: elias@cyberdb.co

Yoel Frischoff, TheRoad

TheRoad (theroadtlv.com) is a strategic branding consultancy, transforming businesses and products.

We build strategies and brands for start-ups reaching scale.

We bring together business strategy and branding, employing a multi-disciplinary approach—facilitating growth and providing guidance in today's ever-changing landscape.

Contact me: yoel@theroadtlv.com

CyberDB
The Cyber Research Data Bank

R

CYBERSECURITY INDUSTRY REPORT

CyberDB
The Cyber Research Data Bank

R

Elias Chachak
elias@cyberdb.co

Yoel Frischoff
yoel@theroadtlv.com