Ovum
TMT intelligence | informa

Ovum Decision Matrix: Managed Security Services Provider Profiles, EMEA, 2018–19

Publication Date: 19 Dec 2018 | Product code: ENS004-000048

Ian Brown

Summary

Catalyst

This report complements the *Ovum Decision Matrix: Selecting a Managed Security Services Provider, EMEA, 2018–19* (aka the MSSP ODM). It provides more detailed profiles of, and comment on, 13 managed security services providers active in the Europe, Middle East, and Africa (EMEA) region. Each profile includes an overview of the MSSP and key events in its history. We highlight the strengths, weaknesses, opportunities, and threats (SWOT) associated with each MSSP, based on the findings of Ovum's MSSP ODM for EMEA, 2018–19. Readers should use this MSSP profiles report to understand why individual MSSPs are classified as market leaders, market challengers, or market followers in the MSSP ODM.

Ovum view

Of the 13 MSSPs in this profiles report, three are classed as market leaders in the MSSP ODM:

- IBM, Secureworks, and Verizon

Six are classed as market challengers:

- Atos, BT, DXC Technology, NTT Security, Orange CyberDefense, and Telefónica

Four are classed as market followers:

- Capgemini, CenturyLink, Infosys, and TCS

The market leaders provide a winning combination of skilled people, efficient processes, and modular, platform-based service delivery. They do not necessarily lead on every single assessment criterion (there were more than 80), but the market leaders are well-placed on the most important criteria.

The overall MSSP ODM results highlight two important factors:

- Today's MSSPs are focused on a platform-based approach to managed security services and delivery.
- Delivering the services customers want from the places customers want them is still work in progress for most MSSPs.

The days of the bespoke, fully outsourced, managed security engagement are numbered. Businesses need to own their IT security, but many have gaps in their in-house IT security capabilities: they need to add functions, but they lack the talent or resources to do so; they need to vet and evaluate technologies, but they do not have the capability; they need to integrate and access external intelligence sources for a full 360-degree view of the threat landscape. These and other requirements underpin the MSSPs' drive to deliver platform-based solutions and services that can be easily integrated with the customer's existing security operations environment.

Delivering the services customers want from the places customers want them is progressing, but at a slower pace than technology development for most MSSPs. Staffing and resourcing security operations centers (SOCs) in places where there is good access to talent at competitive rates remains an expensive business. However, it is an investment that MSSPs must make if they are to meet the needs of their customers.

Key messages

- For the *Ovum Decision Matrix: Selecting a Managed Security Services Provider* reports, Ovum assessed leading MSSPs on three dimensions: portfolio, execution, and market impact.
- For the portfolio assessment, Ovum assessed the MSSPs on their vision for managed security, the scope of their managed security portfolio, their differentiating intellectual property and competency in building IT security solutions, their service portfolio roadmap, the comprehensiveness of their current MSS platform, and their status with, and relationship to, security technology partners.
- For the execution dimension, Ovum considered the effectiveness of the MSSPs' go-to-market strategies; their willingness to seed and develop the market for managed security; the maturity of their MSS engagement models; the reputation of their people and processes; their regional, global, and local service delivery capabilities; the suitability of their MSS governance models; and their competitiveness in the enterprise market.
- Market impact is intended to measure an individual MSSP's current success in the market: How is it perceived by potential customers, competitors, and partners? How successful is it in revenue terms and enterprise market share? How fast is it growing? How significant a player is the MSSP in the regional market and in key vertical industries?
- The *Ovum Decision Matrix: Managed Security Services Provider Profiles* reveals how each of the 13 MSSPs in the EMEA edition of the MSSP ODM performed on the assessment criteria across each of the three dimensions.

Recommendations

Recommendations for enterprises

Enterprises that have difficulty expanding their security operations to deliver trusted and compliant operations in the cloud, or those that struggle to identify and deploy new technologies that can help them prevent or reduce the time to recover from unforeseeable data breaches, should consider the services on offer from the MSSPs included in our MSSP ODM.

Cybersecurity talent and skills are becoming increasingly difficult to find and retain at a time when enterprises are ingesting and retaining more data than they will ever use as they digitize processes and the internet becomes their primary B2C and B2B business channel. Internal resources may be stretched to the limit as digital transformation increases the attack surfaces to be monitored and massively ramps up the volume of network and data activity to be monitored. Service providers are dependent on discovering and nurturing talent. Cybersecurity skills must evolve to keep pace with the increasing sophistication of the attacks and their perpetrators. Securing the enterprise and protecting its data often require the skills of data scientists as well as security analysts, but most enterprises need their data scientists for other tasks that are core to their business.

The lack of expertise and use of resources for non-core tasks are classic reasons for outsourcing IT functions. The difference this time is that MSSPs are targeting discrete functions and services (such as user/entity behavior analytics, managed detection and response, and advanced SOC services) that enterprises can pick and choose from. However, those discrete functions and services must be easy

to integrate with the customer's existing tools and processes, and they must provide a fully architected and integrated SOC/security information and event management (SIEM) solution for those who want it. MSSPs have consequently almost universally adopted a modular platform-based approach to service delivery. Ovum's MSSP ODM reports assess the MSSPs' vision, roadmap, and the maturity of their offers, in tandem with the resources they are deploying to tailor outcomes to customers' needs.

Recommendations for service providers

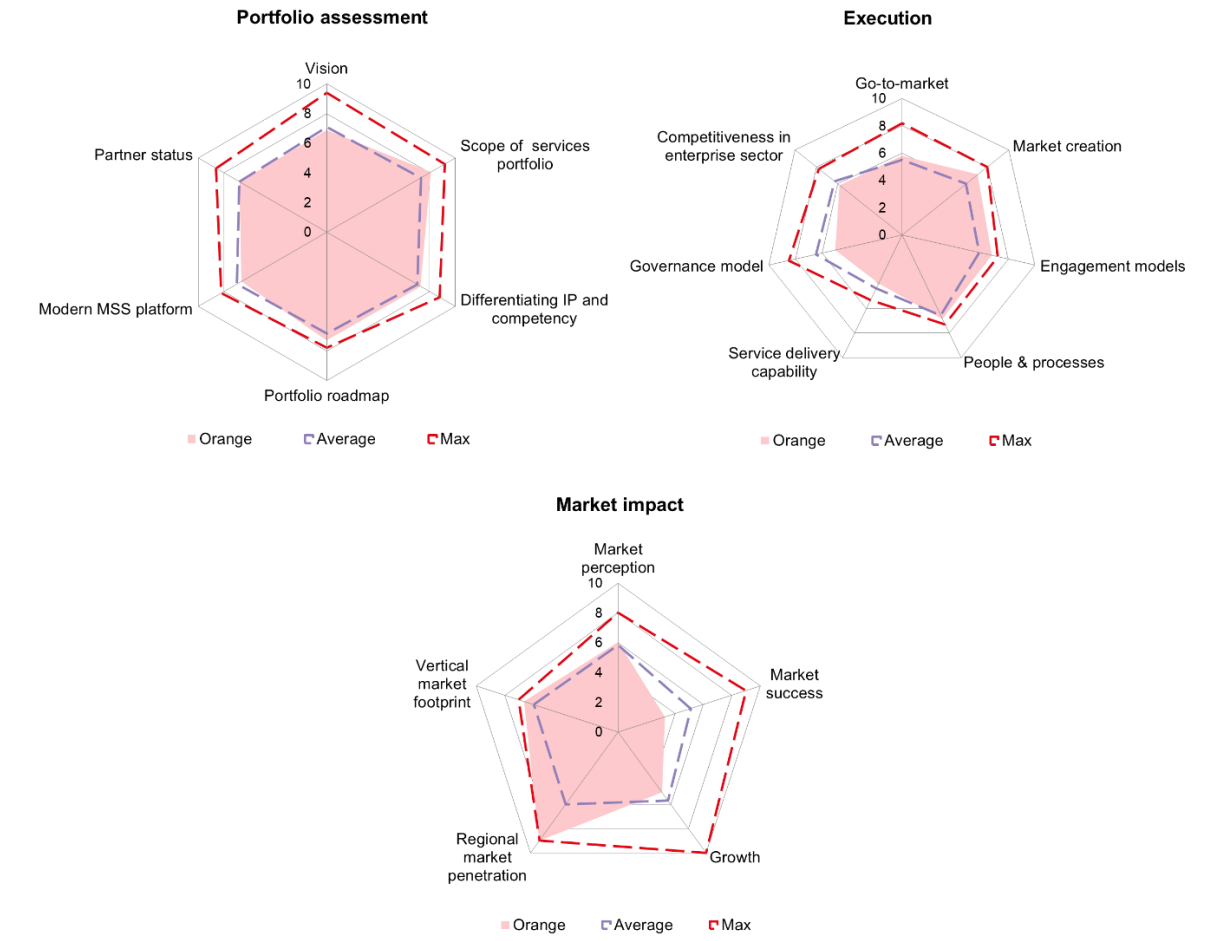
MSSPs should use the ODM profiles to understand where Ovum ranks them on the various criteria we consider pertinent to becoming a successful MSSP. Ovum has positioned itself as an impartial observer of the managed security market. We made the same requests for information (RFI) to all participants and gave them the same opportunities to respond. We listened to enterprises and customers to understand their expectations and IT security priorities. We then assessed the MSSPs' RFI responses through the lens of customers' expectations and responses, as well as what we have learned about industry trends.

The market challenger and market follower MSSPs should understand that the market leaders not only score well on the criteria that are important to enterprise customers, but they also offer the most coherent and intelligible messaging about their managed security strategies. Market challengers and followers need to consider what messages they convey to the market and the extent to which they have become influencers in the managed security services market.

MSSP profile

Orange Cyberdefense (Ovum recommendation: Challenger)

Figure 9: Orange radar diagrams



Source: Ovum

Orange Cyberdefense (OCD) is a dedicated business unit within the Orange Group. It used to be held within Orange Business Services (OBS), but since May 2018, it has been held as a separate entity called Cyber Security and Strategy. Cyber Security and Strategy brings together Orange's internal security teams and the commercial Cyberdefense business in the same organization. The reorganization was designed to ensure greater flexibility for the telco's security investments and to encourage cross-fertilization between internal security teams and the commercial B2B business. Security is considered a major growth area for the Orange Group, and the organization is targeting both organic and inorganic growth. By establishing OCD as a separate entity with its own go-to-market, Orange intends to develop the brand as a pure-play cybersecurity provider beyond the realms of network security.

Orange Cyberdefense's evolution owes much to acquisition and investment. The business unit was formed in January 2016 by consolidating Orange Business Services' security activities with various

security-related acquisitions. Acquisitions that have played an important part in OCD's evolution include the following:

- Atheos, a French security management company, specialized in IAM and SIEM integration. Atheos was acquired in 2014. OBS subsequently initiated a reverse takeover by making the CEO of Atheos the CEO of OCD.
- Lexsi, another European cybersecurity firm based in France, was acquired by OCD in April 2016. Lexsi was a well-recognized computer emergency response team with expertise in security consulting, auditing/penetration testing, incident response, and threat intelligence. Lexsi added 170 cybersecurity experts to OCD and had more than 400 active customers in Europe at the time of its acquisition.

In 2016, Orange Digital Ventures, the Orange venture capital fund, also invested in SecBI, an Israeli startup specializing in AI-powered advanced threat detection. Other recent investments include Morphisec in 2018, which has developed an innovative endpoint threat protection solution, and Alsid, a French startup offering real-time protection for Active Directory services.

OCD has four advanced CyberSOCs: two in France, one in India, and one in Poland. It also has shared SOCs that operate 24x7x365 in Europe (two in France, one in Belgium, and one in Poland), and one in each of the following countries: Egypt, India (covering APAC and the Americas), Malaysia, Mauritius, and the US (Atlanta). More than 85% of OCD's customers are headquartered in EMEA. Its main target markets are France, the UK, Germany, the Netherlands, Switzerland, Australia, and Singapore. OCD has a large base of enterprise and MNC customers, but it also has tens of thousands of SME customers, primarily in France. It is looking to expand its presence in the SME market in countries where Orange has a domestic presence as a local operator.

Most of OCD's managed security services are delivered remotely from its SOCs, rather than on-site at customer premises. The main exceptions are defense, public sector, and companies considered "critical infrastructure operators" under French law. These companies are subject to stringent security rules, and OCD has the appropriate accreditations to work with them.

One of OCD's strengths is that it is a local European provider for most of its customers but has the footprint and global presence of a global telecoms operator. That gives OCD the ability to track, monitor, and identify threats at the global level, which can be critical in warning customers that do not otherwise have visibility into such threats. Threat detection, threat intelligence, and incident response are thus key services required by mature industry sectors, such as banking, insurance, and energy, that tend to have their own SOCs, but need the additional insights.

OCD is also seeing growing demand for IT security services in the manufacturing sector. However, according to OCD, the manufacturing sector's security operations are generally less mature than those of the banking, insurance, and energy sectors. Manufacturing customers often do not have a SOC and most are looking for managed SIEM or cyber-SOC services, security incident detection, and identity and access governance. OCD is also finding strong demand for industrial control system and operational technology security. The MSSP says that almost all customers are looking for solutions to secure Microsoft Office 365, AWS, and Azure.

ODM assessment

Orange has invested heavily in cybersecurity, IoT, and cloud, and that is reflected in its ODM scores on the portfolio assessment dimension. It has brought in the skills and expertise necessary to

establish a broad portfolio of managed security services and to focus on the key elements of threat intelligence, analytics, automation, and response. This is reflected in OCD's above-average scores for scope of services portfolio and portfolio roadmap. OCD has four dedicated computer emergency response teams – two in France, one in Canada, and one in Singapore. Consequently, OCD is reasonably well-placed on four of the six portfolio assessment criteria: vision, scope of security services, portfolio roadmap, and modern MSS platform.

OCD is also well-placed on the ODM's execution criteria, with above-average scores on go-to-market, market creation, engagement models, people and processes, and competitiveness in the enterprise sector. In Ovum's view, its lower positioning on service delivery and governance is largely associated with OCD's maturity as an MSSP delivering services beyond the network level and moving up the IT stack. While OCD is well-regarded for its ability to orchestrate across internal teams as well as third parties, Ovum believes the best-in-class MSSPs combine flexible service delivery, how and where the customer wants, with a high level of customer intimacy and trusted advisor status. Nevertheless, OCD is building its reputation beyond the network level, and recent competitive wins against North American and local French providers go some way to make up for the limited references compared to some of its more mature competitors.

Ovum SWOT assessment

Strengths

- **Orange is a well-known brand and very close to its European customers:** OCD knows its customer base very well through its mobile and business services (OBS) divisions.
- **OCD has a strong focus on intelligence-driven services and incident response:** OCD has expanded its threat intelligence and incident response capabilities through acquisition and investment, and it benefits from the telecoms company's global presence.
- **Many of OCD's core services can be delivered as-a-service or as a managed cloud service:** OCD's Flexible Security Platform provides a portal that enables customers to subscribe to additional services (intrusion detection, sandboxing, identity and access management, etc.). Flexibility and easy access to services are key differentiators in OCD's services portfolio.

Weaknesses

- **Limited brand awareness:** Although part of a telecommunications operator with worldwide operations, OCD's limited brand awareness in markets outside EMEA makes it difficult to attract cybersecurity talent without resorting to acquisition. This is the main factor impacting OCD's global growth and its ability to position itself as a full-service security services provider outside of its core markets.
- **Limited scale and resources outside EMEA:** OCD's scale and resources outside EMEA are limited compared to those of its competitors. For example, OCD lacked a shared SOC in North America until the first half of 2018. The availability of a North American SOC will increase OCD's attractiveness to EMEA customers with operations in the region, but the delay in establishing onshore cybersecurity resources in the region was a limiting factor for some customers.

Opportunities

- **Use acquisitions and capital investment to boost position in global market:** Orange has successfully used the acquisition of local French cybersecurity businesses to establish OCD's position in the European market. With the help of these acquisitions, OCD has developed a comprehensive portfolio of end-to-end services, specializing in mobile, cloud, and IoT security. As network technology changes and customers in sectors such as manufacturing take on IoT, OCD should use acquisition and Orange's venture capital fund to become more of a global player.
- **Build up the midmarket customer base:** As OCD industrializes its services and makes more of its services available in the cloud, the MSSP has an opportunity to build up its customer base in the midmarket. Now that OBS is cloud-agnostic and partners with Microsoft and AWS, OCD should exploit its ability to sell security services as a part of a "security services wrap" to midmarket and other cloud customers.

Threats

- **Challenge from larger global competitors:** OCD, like other MSSPs that are well-known regionally but lack the scale of their global competitors, will face challenges from established global competitors. MSSPs that have a more global service delivery footprint and resources and that position managed security within a continuum of cybersecurity services will appeal to the needs of MNCs operating in two or more regions.
- **Local and regional managed services providers:** At the other end of the scale, local and regional competitors that offer modular, cloud-based security services as complementary options to their managed services offer are specifically targeting midmarket customers that are moving more of their IT operations to the cloud.

Appendix

Methodology

There were five stages to the research for *Ovum Decision Matrix: Selecting a Managed Security Services Provider, EMEA, 2018–19*:

- Each MSSP included in the report was asked to complete a structured request-for-information questionnaire.
- Each MSSP was invited to provide a briefing or presentation on its MSS offering.
- Ovum made follow-up calls to MSSPs for clarification of their responses and contacted managed security services customers for additional insights into their service providers.
- We then scored each MSSP on nearly 80 elements, grouped into 17 criteria across three dimensions: portfolio assessment, execution, and market impact.
- We applied weightings to each of the criteria and to the three dimensions to reflect the importance Ovum ascribed to them in terms of customer wants and needs.

The scores and report write-up were subjected to internal peer review. Individual profiles in the *Ovum Decision Matrix: Managed Security Services Provider Profiles, EMEA, 2018–19* report, which forms part 2 of the ODM, were submitted to the participating MSSPs for fact-checking.

Further reading

Ovum Decision Matrix: Selecting a Managed Security Services Provider, EMEA, 2018–19, ENS004-000046 (November 2018)

Ovum Decision Matrix: Selecting a Managed Security Services Provider, the Americas, 2018–19, ENS004-000045 (November 2018)

2018 Trends to Watch: Managed Security Services, TE0005-001001 (September 2017)

"Not all security providers are made equal," INT003-000250 (October 2018)

Author

Ian Brown, Senior Analyst, Network Transformation and Cloud

ian.brown@ovum.com

Mike Sapien, Chief Analyst, Enterprise Services

mike.sapien@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo