Market Guide for Managed Detection and Response Services, China

Published 17 October 2022 - ID G00764382 - 21 min read

By Analyst(s): Angela Zhao

Initiatives: Security Operations

> Managed detection and response continues to be one of the top security services that China organizations invest in. Security and risk management leaders in China should use this research to understand China's MDR market and its dynamics.

Overview

Key Findings

- Due to various customized user requirements, managed detection and response (MDR) services in China have evolved with a large set of categories supporting a range of use cases, beyond threat detection and response. Organizations struggle to select the most suitable service items from the long catalog of MDR services.
- Remote MDR services with provider-owned technologies are not widely accepted in China yet. Plus, the IT environments are getting more complicated, with hybrid cloud, multicloud and cyber-physical systems (CPS). These create complexity and options for users of MDR services, in terms of service delivery models and technology coverage.
- The deliverables and corresponding performance of MDR services varies from provider to provider, but there are no commonly accepted SLA standards in the market to help buyers perform a fair comparison and ongoing vendor management.
- Many MDR services in China are focusing on monitoring and detection rather than response (containment and mitigation) to reduce the risks and impacts of security incidents.

Recommendations

To optimize their use of MDR services, security and risk management leaders in China should:

- Use core MDR services to obtain in-depth threat detection and response capabilities, and purchase only the needed adjacent services based on your organization's requirements to avoid overinvestment.
- Investigate MDR providers' abilities to ensure they fit your organization's existing technology investment, in-house capabilities, compliance restrictions and technology landscape.
- Establish SLAs and conduct continuous evaluation of service levels to ensure continuous improvement of the overall maturity of security operations.
- Ensure your MDR provider has effective security containment and response of threats through the MDR service's incident response capabilities, processes and integration with IT ticket systems, and trust the provider to take active response actions.

Strategic Planning Assumption

By 2026, 60% of organizations in China that currently have an internal security operations center (SOC) will use MDR services to augment their internal security capabilities and resources.

Market Definition

MDR is defined internationally as the services providing customers with remotely delivered modern security operations center (MSOC) functions. These functions allow organizations to rapidly detect, analyze, investigate and actively respond to threat mitigation and containment. MDR service providers offer a turnkey experience, using a predefined technology stack that commonly covers endpoint, network, logs and cloud. This telemetry is analyzed within the provider's platform using a range of techniques. This process allows for investigation by experts skilled in threat hunting and incident management, who deliver actionable outcomes.

Market Description

Within the China market, MDR services are delivered differently because China buyers are well-positioned to implement customized requirements and specific constraints, in accordance with local laws and regulations. MDR services in China are different from those of the global market through their hybrid delivery model of combining remote and on-site service teams and the various options of adjacent services that are available.

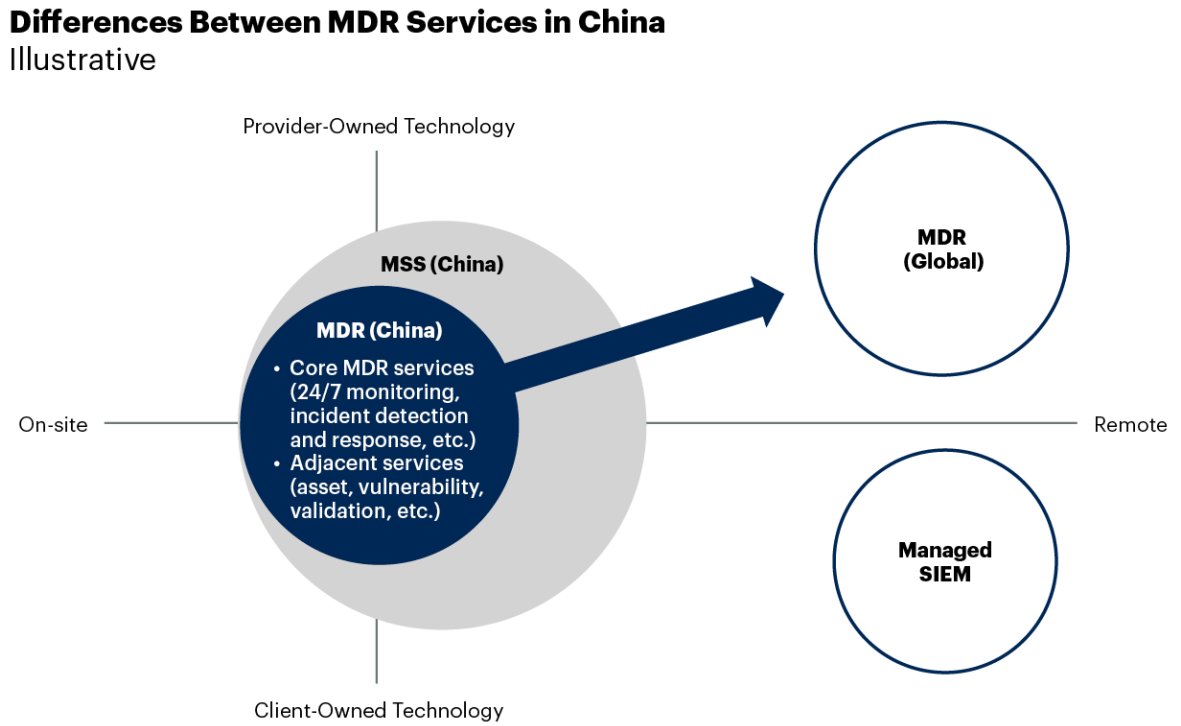
China's MDR services market is composed of providers delivering 24/7 threat monitoring, detection and response outcomes. MDR services collect telemetry from various devices in the customer's private network and cloud-based infrastructure. Security analysts monitor client data and alert 24/7 to identify active security threats through the detection of abnormal behaviors and known tactics, techniques, and procedures. MDR services should also be able to respond in real time as much as possible. They should also be able to perform automated or manual containment or remediation actions on behalf of the customer where appropriate, supporting the customer to take remedial action with suggested measures. Some threats may need to be flagged for further investigation by 24/7 experts before entering the remediation phase.

MDR services in China are different from the global definition with below specific attributes:

- **Most vendors deliver the services in both width and depth** — various adjacent services are available and are usually bound with the core MDR services. This is mainly because buyers in China expect that MDR services not only monitor and respond to threats, but also provide knowledge and competencies to mature their processes and form a closed loop of prevention-detection-response-prediction. The adjacent services around assets, vulnerability, validation and the like are also highly welcomed in China.
- **Flexible delivery models** — They provide customers with a flexibility to choose delivery models in terms of technology stack ownership and delivery location. But the centralized monitoring and analysis is always done by the MDR service provider, and remotely in most cases.
- **Various names** — Due to language differences, China's MDR services often go by many names besides MDR, such as managed security services (MSS), security operation services and managed SOC, though the functions and scope are quite similar across different vendors' offerings.

China buyers should be aware that MDR services are designed to deliver more "out of the box" operational efficiencies with minimal customization, and are in a remotely delivered, shared model that is easy to consume. Most MDR services in China today are not strictly MDR, but also general security services. However, we have noticed they are moving forward to the international model, due to the influence of COVID-19 (on-site delivery is not possible under lockdowns) and cloud adoption. Figure 1 illustrates the differences between MDR services in China, international MDR services and managed security information and event management (SIEM) services.

Figure 1. Differences Between MDR Services in China



Source: Gartner
Note: MDR = Managed detection and response, MSS = Managed security services, SIEM = Security information and event management
764382_C

Gartner

Market Direction

Compared with the other types of security services that are more mature in China (e.g., consulting), the MDR services market is still in a stage of expansion in China, so it has huge potential for growth. The frequent large conferences and events in China also drive this market, as it is easier to purchase detection and response capabilities via a service consumption model than to deploy technologies directly for only a short period.

The development focus of China's MDR market is different from that of the rest of the world. In the past, in order to obtain a continuous and integrated security operation capability, organizations with insufficient headcounts and funds, but with high demand for security, often only had the option to purchase on-site security operations services. In these cases, "visible" on-site service was preferred by many organizations. However, this face-to-face approach has gradually revealed its drawbacks under the scenarios of the COVID-19 pandemic and advances in technology, not to mention its higher cost. In the past two years, many organizations have realized that they are not able to purely rely on on-site services due to the lockdown and quarantine policies during the pandemic. They have begun to seek automated, remote and fast-to-deploy security operations solutions. As a result, MDR services have developed in China and become the top choice for many organizations looking to establish more-mature security operations functions quickly and effectively.

Different types of organizations have different requirements and expected outcomes of MDR services. Small and midsize businesses without sufficient security foundations (headcount, technology deployment, etc.) want MDR services to quickly deliver basic monitoring and response functions, to meet security baselines from regulations and standards such as multilevel protection scheme (MLPS) 2.0, and to respond to security incidents that are not expected to occur frequently or with huge impacts. Large organizations that have deployed a number of security devices are facing an increased number of security alerts and incidents, low efficiency and high false-positive rates. They expect MDR services to consolidate and streamline security operations across different technologies to have faster and higher efficacy of threat detection, focus on protection of the most valuable assets, provide automated response/mitigation/closure of noncritical security alerts, and quickly involve security experts for critical incidents.

With the government's emphasis on controllable cybersecurity, Chinese organizations will use a large number of domestic information technologies due to the Xinchuang initiative (Chinese-language link; see also Note 2) in the future. This initiative requires MDR service providers to have compatibility with domestic technologies and environments (collect logs, parse and analyze to detect security abnormalities and incidents), especially if their target clients are local organizations.

Buyers are not just satisfied with monitoring and analysis capabilities from MDR service providers, but also expect that a valuable MDR service can find the root cause of a detected security event and propose actions to the right people as soon as possible, so that remediations (e.g., policy changes, software updates, network access blocks) can be made immediately.

Market Analysis

Avoid Packages — Select Only the Adjacent Services You Need

The needs of Chinese customers can often be different than in other regions. They are often subject to stronger supervision and oversight by national government and industry regulators, and there is a different domestic threat landscape and trajectory of internetization and digitalization. On the other hand, in keeping with the global talent shortage, most organizations in China have insufficient cybersecurity personnel and skills. Commonly delivered and repeatable core MDR services often cannot satisfy such complex scenarios, but an overall service mechanism is required. In some cases, providers have opportunistically evolved their offerings to cater to diverse customer needs. As a result, there are many service items available for customers to choose from. See Table 1 for an example of common MDR service items. In order to simplify customer choice, many service providers have developed different service packages (such as basic, optimized, advanced, etc.), and then add relevant additional items as needed.

Table 1: Examples of MDR Service Items

(Enlarged table in Appendix)

Area	Items
Core MDR services	■ 24/7 monitoring ■ Incident detection ■ Incident response (investigation, containment, remediation) ■ Threat intelligence ■ Threat hunting

Adjacent services	■ Asset discovery and management
	■ Vulnerability assessment
	■ Forensics
	■ Incident root cause analysis
	■ Validation
	  ■ Attack and defense teaming
	  ■ Penetration test as a service (PTaaS)
	■ On-site support
	  ■ On-site special protection during important periods
	  ■ On-site emergency response
	  ■ Other on-site support

Source: Gartner (October 2022)

Fully remote MDR services are not widely accepted in China yet, especially for large organizations who still want to have on-site personnel. Compared with the remote team that is shared by multiple organizations, the on-site team would have more familiarity with the customer's environment, as well as more frequent and efficient communication with the customers. However, organizations need to understand whether this is already included in the service fee or carries an additional charge. Organizations still need to consider factors such as travel time and cost and quarantine policies, and therefore should continue to explore elastic, flexible, remote MDR services that meet the needs of the organization.

When organizations choose MDR services, it is understandable that they would have different perspectives and interpretations of the same type of services due to the use of different terminologies and vendors' individual marketing language. Using the strict definition of MDR, we can see that MDR is providing customers with the expertise, processes and technologies associated with security operations functions in a turnkey and repeatable way, delivered remotely. Therefore, buyers should make sure to ask MDR providers which functions their own security team should cover versus which functions the service providers will perform. For more information, see What Makes a Successful Security Service RFP?.

Besides service items, other key factors to consider are the characteristics of your organization's businesses and IT environment. For example, large government and enterprise or smart city operations may pay more attention to the actual security efficacy of an MDR service provider — whether they can quickly alert and respond to targeted attacks, and link information and tools in a complicated and multilevel organizational structure. And validation services may not be as attractive to them. Industrial manufacturing organizations usually have a weaker IT foundation, a more-limited IT security investment and team size, and heterogeneous data sources, so they will likely care about whether MDR service providers can cover the operational technology/Internet of Things (OT/IoT) environment and have strong capabilities about threat containment to resume production from security incidents.

In addition, every organization has its own budget constraints, and different organizations have different compliance needs and risk management realities. Organizations need to find an MDR vendor within budget, and at the same time, they need to be able to fill the gaps in the capabilities of their internal team based on their existing architecture, technology stack and the critical threats they face. Along with environment and business change, organizations also need to ensure there are flexibilities in the MDR service delivery and the scope; adjacent services can be expanded or reduced according to business needs.

Find MDR Providers That Fit Your Organization's Delivery Model and Technology Environment

A turnkey technology stack on a shared platform is a key feature of MDR services. However, many organizations in China expect the MDR service provider to offer more flexibility, either due to existing investment of technologies, compliance restrictions associated with using MDR services on a public cloud, or sensitivity of the security information. As a result, many China MDR service providers have begun to explore flexible delivery models to adapt to local market and customer requests.

From the perspective of technology deployment, MDR services can provide the following choices for customers (see Table 2):

Table 2: MDR Delivery Models in China

↓	*Owned by the MDR Provider* ↓	*Owned by the Customer* ↓	
Full Technology Stack From the Provider	Full SecOps technologies		Infrastructure and other security tools
Bring Your Own (BYO) Technology Stack	A few SecOps technologies (e.g., TI)	Most SecOps technologies	Infrastructure and other security tools
Hybrid Technology Stack	Some SecOps technologies	Some SecOps technologies	Infrastructure and other security tools

Source: Gartner (October 2022)

1. **Full security technology stack from the provider.** MDR service providers use their own curated technologies to provide organizations with detection and response capabilities, such as situational awareness platforms, threat intelligence and the like. Organizations that have a very small toolset of secure operations, or want to change their existing security tooling, can prioritize this model. However, not all vendors have the capabilities to offer a full security technology stack.

2. **Bring-your-own technology stack.** This is a traditional, but still common approach, where the MDR service provider works with the tools that the organization has already deployed, and supplements required tools (on either a purchase or rental basis) where needed. This is a preferable method for organizations that have deployed a large number of security tools, or those that have strict restrictions on cloud usage, as many MDR service providers are using cloud as their technology platform.

3. **Hybrid.** At present, MDR service providers in the China market are beginning to explore the hybrid method as a combination of the above two models. This works for organizations that have already deployed some security operations tools and want to supplement or enhance their threat detection and response capabilities through MDR service provider technology. Organizations can effectively integrate their own security operations tools and MDR service provider platform through APIs or other integration measures, like an IT service management tool and collaboration tools.

Even with special requirements from buyers in China, it is essential that the core monitoring and analysis of MDR services be conducted remotely.

Cloud adoption brings a new problem to buyers: choosing between different types of MDR service providers. Cloud service providers are stepping into the market. They mainly focus on the security operation of the public cloud environment, provide operations and monitoring services for cloud products, and have stronger capabilities in terms of cloud-native security. Traditional security companies have more advantages in security technology, security service talents, and operational processes due to their rich experiences in the field of cybersecurity.

With the promotion of smart cities in China's 14th Five-Year Plan, some organizations are facing security threats in not only IT systems, but also CPS. For these organizations, they need MDR services that can not only monitor IT, but also can detect attacks and security incidents unique to CPS, due to special protocols and an industry-specific threat landscape.

For organizations with a complex technology environment, it is important to examine whether the MDR service can solve the following problems to provide end-to-end security:

- **Visibility and compatibility**: MDR solutions should be able to break through the limitations of monitoring different environments, and achieve full visibility into data center, cloud, and CPS environment resources and services. But this does not mean that a set of security tools must be compatible with all different infrastructures. MDR service providers may make different tools responsible for different environments, and then integrate security data together to achieve a holistic view of security events.

- **Multienvironment deployment:** MDR solutions should be easy to deploy in different environments and can be up and running quickly. When customers need rapid cloud or digital development, security services should not be a factor that hinders speed, but should be prepared in advance and become a help to guide the direction of business and IT development.

Use Quantifiable SLA to Evaluate MDR Service Quality

A common standard of SLAs is the ability to deliver IT services on a large scale. However, from the top-down perspective, the government and regulators have not yet issued MDR service evaluation standards that address the general needs of the market. Therefore, the purchasers of MDR services are mainly relying on brand recognition (e.g., whether the MDR service provider has a security operations service certificate, and at which level) and past compliance with government standards. It is difficult for organizations to quantify the quality and delivery results of MDR services during procurement and service delivery.

Organizations should evaluate the ability of MDR services to recover critical business applications from security incidents in accordance with desired recovery time objectives (RTOs) and recovery point objectives (RPOs). At present, many MDR service providers in the China market have begun to proactively provide SLA suggestions, but most indicators currently use time as the only measurement, such as mean time to detect (MTTD) and mean time to respond/contain (MTTR/C). These SLAs are important, but have disadvantages if they are the only ones being used. During the service delivery, the MDR service provider may sacrifice quality to meet the time requirements to try and make a metric look good, or transfer some more complex and time-consuming work (such as detailed investigation of incidents) to the organization's internal team. Therefore, organizations still need to complement other types of SLAs (such as accuracy of incident identification and actionable recommendations of remediation) to ensure MDR services to generate real benefits. See Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security.

Furthermore, a stricter SLA is not necessarily a better one. Usually, the higher the service level, the higher the cost. Organizations should balance risk and cost to choose the SLA that best suits their goals.

Some Chinese organizations are experiencing an issue when evaluating service performance: they focus too much on people (number of people, working experiences, etc.) rather than the overall outcome and quality of the service. It is true that MDR services rely heavily on experienced security experts, but buyers should also be aware that those experts are shared and reusable. Organizations should shift their mindsets away from focusing on team size, individual performance and working hours, and instead evaluate the whole MDR service from a results-driven perspective.

Rapid and Effective Response Should Be Addressed by MDR Services

Many MDR services in China today are mainly focused on threat detection and analysis, with very limited response deliveries. This is due to several reasons:

- Incident response and remediation is time-consuming and requires different levels of verification by MDR service provider experts. However, some MDR service providers lack experienced security experts, just like end users are seeing staff shortages.
- MDR service providers do not have an in-depth understanding of the organization's business processes and IT processes, and cannot provide targeted response suggestions for the organization, much less directly perform containment actions.
- MDR service providers do not have sufficient access rights to internal systems, so they cannot directly and quickly take actions (e.g., containment, change configurations) on the infrastructure or other security devices that they do not own.
- The MDR solution is not highly automated and lacks coordination to accelerate the incident response activities remotely.

The response is a key area for improvement. Organizations should carefully investigate MDR service providers' response capabilities during vendor selection, using RFP and a proof of concept and requesting sample deliverables. At the same time, organizations should not have unrealistic expectations for MDR service providers (especially at the price point of many MDRs), and be aware that the final accountability is always with the organizations but cannot be outsourced.

A clear roles and responsibilities mechanism is necessary to enhance the incident response capability, and it is here where you can also evaluate the need (or lack of need) for an MDR for your organization. Your organization should identify which scenarios (incident level, mitigation action type, impact, etc.) can be handled by the MDR service provider on behalf of your internal security operations team, and then fully and formally authorize the MDR service provider in terms of responsibilities and access rights to required systems. The organization can also establish some simple approval and initiation mechanisms and maintain a higher degree of flexibility in daily operations. This requires the organization to have a more mature incident-handling process.

MDR service providers will never replace the internal team. Even if the MDR service provider has industry experts, the differences in the internal organizational structure, business process and system architecture of each organization will result in different threat landscapes, vulnerabilities and stakeholders. In fact, security operations, especially incident response and mitigation, always require the participation of internal teams. In a well-staffed organization, the internal security team can take responsibilities and negate the need for an MDR as they are essentially delivering MDR already, with the organization as the only client. Organizations with a shortage of internal staff should also have at least an officially authorized contact person as a bridge among the MDR service provider, business departments, IT department and other IT service providers.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

Table 3: Representative Vendors

(Enlarged table in Appendix)

Provider	Service Name [1]	Headquarters
360 Digital Security Group	MSS托管安全运营服务	Beijing, Beijing, China
Accenture China	托管安全服务	Shanghai, China
Alibaba Cloud	安全管家服务	Hangzhou, Zhejiang, China
Antiy	常态化安全运营服务	Harbin, Heilongjiang, China
Atos Information Technology (China) Co., Ltd.	MSS安全托管服务	Beijing, China
Capgemini China	安全运营中心服务	Shanghai, China
DAS-Security	安全托管运营服务	Hangzhou, Zhejiang, China
Deloitte China	MSS安全托管服务	Shanghai, China
Hangzhou DPtech Technologies	威胁检测与响应服务	Hangzhou, Zhejiang, China
H3C	威胁检测与响应服务	Beijing, China
Huawei	安全云服务	Shenzhen, Guangdong, China
NSFOCUS	一体化安全运营服务	Beijing, China
PwC Mainland China	安全托管服务	Shanghai, China
QI-ANXIN Technology Group	安全托管服务	Beijing, China
Qingteng Cloud Security	主机安全运营服务	Beijing, China
SafeDog	安全托管服务	Xiamen, Fujian, China
Sangfor Technologies	托管检测与响应服务	Shenzhen, Guangdong, China
Tencent Security	安全托管服务	Shenzhen, Guangdong, China
ThreatBook	MDR检测及响应服务	Beijing, China
TOPSEC	安全运营服务	Beijing, Beijing, China
TYUN	安全运营服务	Shanghai, Shanghai, China
Venustech	安全托管业务	Beijing, China

[1] Some service names are not called MDR, either due to translation difficulties or because MDR is one subcategory/package within an overall security operations service.

Source: Gartner (October 2022)

Market Recommendations

Security and risk management leaders in China should:

- Define their organization's roadmap of security investment — balance between MDR services and on-premises technologies. Consider more services and renting technologies if you lack internal expertise to deploy, maintain and operate security technologies and processes.
- Evaluate MDR services not by brand, but by their organization's unique needs, and then select what can enhance or augment their SOC capabilities from the menu of services.

- Define the most suitable service model for their organization before procuring MDR services, according to their existing technology investment, in-house capabilities and compliance restrictions.
- Investigate MDR service providers' capabilities to support cloud, OT, or IoT if their organization has such needs and consolidate data for an overview across different environments.
- Mitigate the risk of underperforming services by negotiating robust SLA terms into contracts, for not only system availability/uptime, but also disaster recovery targets (RTOs/RPOs) and support ticket resolution for business-critical applications.
- Incorporate the service-level reporting process into the contract, and delegate ownership of ongoing service monitoring by the appropriate teams within their organization.
- Update their incident response processes and procedures to include the MDR service provider with clearly defined responsibilities. They should also set up and continuously fine-tune the collaboration model between the MDR service provider and their internal team for incident reporting, handling and remediation.

Note 1: Representative Vendor Selection

Gartner has included a range of providers in this research to ensure coverage from a geographical, vertical and capabilities perspective. Gartner estimates that more than 50 providers in the China market claim to offer MDR services. Listed here are those that are visible to Gartner clients based on inquiries and represent variety in both distribution and size. This is not intended to be a list of all the providers in China's MDR services market. It is not, nor is it intended to be, a competitive analysis of the providers.

Note 2. Main Technology Sectors in the Xinchuang Initiative

Main technology sectors in the Xinchuang initiative include:

- Hardware: chips, storage, complete machines and the like
- Software: operating systems, databases, middleware, office software, industrial applications and similar
- Cybersecurity technologies and services
- Cloud services

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Market Guide for Managed Detection and Response Services

Market Guide for Managed SIEM Services

Market Guide for Managed Security Services

Quick Answer: What Key Questions Should I Ask When Selecting an MDR Provider?

Quick Answer: How Do I Manage the Risks Associated With Outsourcing to an MDR Provider?

Top Practices for Security Operations in China

Table 1: Examples of MDR Service Items

Area	Items
Core MDR services	■ 24/7 monitoring ■ Incident detection ■ Incident response (investigation, containment, remediation) ■ Threat intelligence ■ Threat hunting

Area	Items

Adjacent services	■ Asset discovery and management
	■ Vulnerability assessment
	■ Forensics
	■ Incident root cause analysis
	■ Validation
	  ■ Attack and defense teaming
	  ■ Penetration test as a service (PTaaS)
	■ On-site support
	  ■ On-site special protection during important periods
	  ■ On-site emergency response
	  ■ Other on-site support

Source: Gartner (October 2022)

Table 2: MDR Delivery Models in China

	Owned by the MDR Provider		Owned by the Customer
Full Technology Stack From the Provider	Full SecOps technologies		Infrastructure and other security tools
Bring Your Own (BYO) Technology Stack	A few SecOps technologies (e.g., TI)	Most SecOps technologies	Infrastructure and other security tools
Hybrid Technology Stack	Some SecOps technologies	Some SecOps technologies	Infrastructure and other security tools

Source: Gartner (October 2022)

Table 3: Representative Vendors

Provider	Service Name [1]	Headquarters
360 Digital Security Group	MSS托管安全运营服务	Beijing, Beijing, China
Accenture China	托管安全服务	Shanghai, China
Alibaba Cloud	安全管家服务	Hangzhou, Zhejiang, China
Antiy	常态化安全运营服务	Harbin, Heilongjiang, China
Atos Information Technology (China) Co., Ltd.	MSS安全托管服务	Beijing, China
Capgemini China	安全运营中心服务	Shanghai, China
DAS-Security	安全托管运营服务	Hangzhou, Zhejiang, China
Deloitte China	MSS安全托管服务	Shanghai, China
Hangzhou DPtech Technologies	威胁检测与响应服务	Hangzhou, Zhejiang, China
H3C	威胁检测与响应服务	Beijing, China
Huawei	安全云服务	Shenzhen, Guangdong, China
NSFOCUS	一体化安全运营服务	Beijing, China
PwC Mainland China	安全托管服务	Shanghai, China
QI-ANXIN Technology Group	安全托管服务	Beijing, China
Qingteng Cloud Security	主机安全运营服务	Beijing, China

Provider	Service Name [1]	Headquarters
SafeDog	安全托管服务	Xiamen, Fujian, China
Sangfor Technologies	托管检测与响应服务	Shenzhen, Guangdong, China
Tencent Security	安全托管服务	Shenzhen, Guangdong, China
ThreatBook	MDR检测及响应服务	Beijing, China
TOPSEC	安全运营服务	Beijing, Beijing, China
TYUN	安全运营服务	Shanghai, Shanghai, China
Venustech	安全托管业务	Beijing, China

[1] Some service names are not called MDR, either due to translation difficulties or because MDR is one subcategory/package within an overall security operations service.

Source: Gartner (October 2022)