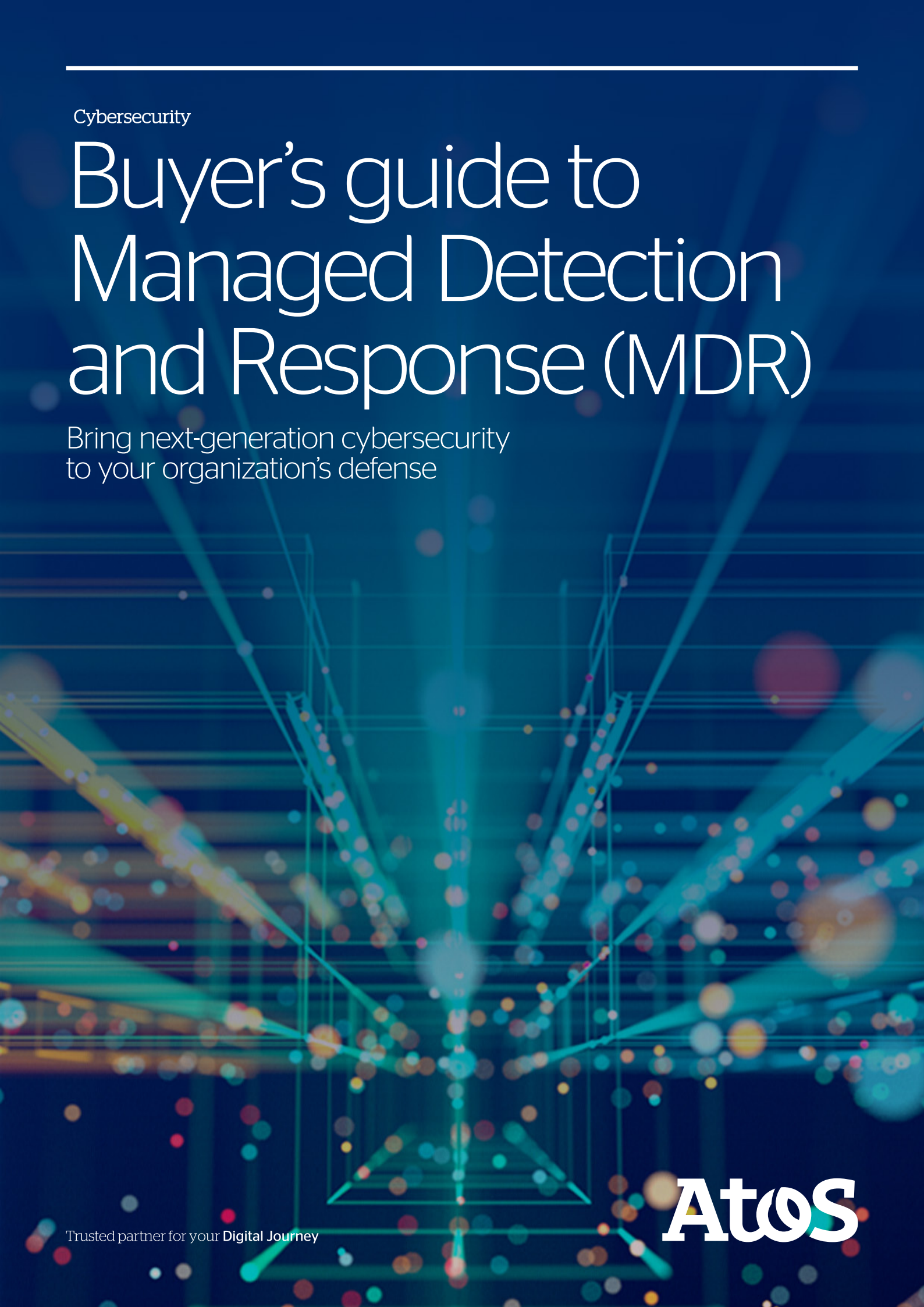
Cybersecurity

Buyer's guide to Managed Detection and Response (MDR)

Bring next-generation cybersecurity to your organization's defense



Trusted partner for your **Digital Journey**

Atos

Content

04 What created this need for MDR?

04 What is it, and why you need it?

05 How to adopt advanced Threat Detection and Response?

05 How to bring MDR to your organization?

06 Is MDR right for your organization?

06 How to select an MDR vendor?

07 Selecting a full-scale MDR partner

What created this need for MDR?

Three primary trends in the security landscape converged to create the need for MDR.

Organizational trends

Security teams and operations were struggling to stay afloat. They could barely keep up with tactical, day-to-day security activities, let alone perform advanced, proactive activities, such as threat hunting. They lacked the skills and staff required to protect their organizations. Next-generation security could no longer be handled "in house" in most organizations.

62-64%

of respondents find that day-to-day tactical [security] activities take up too much time, and lack sufficient security team staff.

Market trends

A new wave of technology outsourcing options and cloud solutions entered the market. Very quickly, most organizations adopted managed services for the majority of their technology needs. Managed security services naturally entered this space, and organizations felt increasingly comfortable adopting managed services to shore up their internal security shortcomings.

64%

of respondents adopted SaaS security services because the rest of their environment is already outsourced.

Tools & technology trends

New tools & technology entered the marketplace, and organizations adopted them at a rapid rate. Many of these tools & technologies fall under the umbrella of "digital transformation," and they all opened up new vulnerability points. For example, organizations began to increasingly invest in endpoint tools and controls, and soon realized they lacked the skills to defend these new endpoints.

61%

of respondents are implementing/expanding implementation of endpoint visibility and control one.[1]

1 Forrester's Global Business Technographics® Security Survey, 2016

What is it, and why you need it?

The three trends described in the previous page created a new landscape that MSSPs can no longer defend. The new security landscape required dedicated Managed Detection and Response (MDR) services centered around new talent.

Gartner defines MDR as:

"Managed Detection and Response (MDR) services provide customers with remotely delivered modern Security Operations Center (SOC) capabilities to rapidly detect, analyze, investigate and actively respond to threats (e.g., containment or disruption). MDR service providers offer a turnkey experience, with many using a predefined technology stack covering endpoints, networks, cloud services, Operational Technology (OT)/ Internet of Things (IoT) and other sources, to collect relevant logs, data and other telemetry (e.g., forensic data, contextual information)."[1]

Forrester defines MDR as:

"A fully managed security service that includes the application of advanced security analytics, proactive threat hunting, and incident response investigative capabilities along with security automation orchestration (SOAR) for automated, manual, and on-demand response actions based on predefined and custom escalation workflows.[2]

[1] Market Guide for Managed Detection and Response Services, 24th Sep 2020

[2] Now Tech: Managed Detection and Response Services Providers, 16th Dec 2020

How to adopt advanced Threat Detection and Response

An effective MDR vendor provides numerous benefits to any organization they partner with. However, there are two critical benefits which most organizations seek and receive when they select the correct partner:

A proactive approach to combating attacks

The traditional MSSP-driven approach to security was primarily reactive. It depended on malicious actors deploying known attacks, which then triggered alerts for further investigation. This approach was never ideal, but it has become increasingly ineffective as most next-generation attacks are unknown, and can compromise an organization without triggering any known rules. By deploying threat hunting—in addition to advanced AI-driven analytics—MDR providers can detect and uncover unknown threats lurking within your network that were undetected by traditional defenses.

Accelerated detection, investigation & response

An MDR provider's proactive approach, on its own, speeds up detection by finding threats before their trigger alerts or cause damages. But, MDR technologies further accelerate detection. When initially deployed, they comb through your system to ensure a previously undetected threat does not already compromise you. They maintain access to your assets, allowing them to investigate any potential threat as soon as it is detected. And they can initiate response as soon as an incident is confirmed, initiating containment, expulsion, and remediation in near real-time.

How to bring MDR to your organization

Switching to MDR-driven defense may feel unnatural to many organizations. Traditionally, organizations handled all security activities in-house or worked with an MSSP firm.

In-house security teams and MSSPs have primarily worked in isolation from each other, with the in-house team sending log information to the MSSP, and the MSSP sending alerts back. By contrast, an MDR provider works much closer, a more intimate partnership with any existing in-house security or MSSP, and often takes on activities such as investigation and response, which was previously handled by a dedicated in-house team or a 3rd party.

In the near future, many organizations will likely take a hybrid approach towards adopting MDR. Rather than contracting a provider for their full service, many organizations are more likely to bring in MDR providers for highly specialized security skills and services, which they cannot perform themselves. These services and skills will extend well beyond a traditional organization/MSSP. Over time, as the volume of services and skills required escalate, the number of organizations adopting more comprehensive MDR services will likely increase.

"Atos AI-driven MDR service has powerfully augmented our existing security posture. They tailored their security services to meet our specific needs and deployed their services quickly and simply. They both increased the speed of our detection and response, and done so with a very high-touch, people-first approach that our internal security team loves."

- CIO, Fortune 500 Manufacturing Company

Is MDR right for your organization?

While MDR services represent the future of cybersecurity, not every organization is currently equipped to get the most value from such a partnership.

Mid-size enterprises and large enterprises derive the most value from these services. This is less due to size and more due to maturity. Low-maturity organizations often lack the telemetry, technology, and processes required to effectively partner with an MDR provider. But once a baseline level of security technology, processes, and activities have been introduced into an organization at a moderate to high level of maturity, a partnership with an MDR provider begins to deliver real results.

How to select an MDR vendor?

Two categories to select your MDR partner

There is no single "best" MDR partner in the marketplace. You must select a partner who best meets the needs of your organization, according to two key categories—security analytics and orchestration capabilities, and what service functionality the partner provides.

Selecting by security analytics and orchestration capabilities is simple: look for a partner that can offer these four security analytics; endpoint, user behavior, application threats, and network threat analytics. The vendor should also be able to provide some response automation for swift threat containment.

Selecting by functionality is slightly more complicated, as different organizations have different security needs, different needs regarding what functions they will handle in-house rather than outsource, and different risk profiles. In a general view, it is wise to determine, before engaging the market of potential providers, whether you simply require a partner to:

- Conduct light investigations via relatively shallow analytics (generally endpoint analytics)
- Accelerate investigation and response within a narrow band of analytics
- Complete investigation and response across your entire organization.

"We had a good handle on all of the normal, known attacks coming our way. But Atos detected threats that no one had discovered yet... including a few threats that had been lurking inside our system for almost a year that our traditional security measures hadn't detected. Since partnering with Atos, we no longer worry about all those "unknowns" threats we didn't we were ignoring."

- Senior IT Director
National Retail Chain

Selecting a full-scale MDR partner

For organizations seeking more comprehensive MDR services (option 3), they must ensure any partner they consider has built their service around the following elements:

Managed detection

To offer true MDR services, the provider must extend their detection services beyond the traditional signature-based detection that most MSSPs have provided for some time now. They cannot merely send alerts from security technology you already have in place. The provider must also apply advanced analytics including AI-deployed machine learning algorithms on a repeatable and scheduled basis. Finally, they must also perform proactive threat hunting, on a similarly repeatable and continuous basis.

Comprehensive MDR framework

The provider must have a fully articulated and deployed framework for detecting and responding to threats at every stage of their lifecycle. While you may have need for only a segment of their services, the provider cannot be considered legitimate if they only offer ala-carte MDR like services. The provider's MDR framework must not only be comprehensive, but it also must be both turnkey and adaptable to existing technology investments to allow for fast, cost-effective deployment.

Managed response

The provider must also offer true managed response services, which typically revolve around the ability to perform automated response actions based on predefined escalation workflows. These workflows must be continuously updated to ensure response processes are optimized and relevant against emergent threats. The exact workflows must also be customized to your organization to ensure their relevance. While the exact workflows and integration will vary, any potential partner must be able to manage response to accelerate threat investigation and remediation.

MDR technology stack

A few technologies must come standard in any top-tier MDR provider. These include monitoring technologies across critical data sources (e.g., endpoint, network, application, and user data), and across multiple infrastructures (including cloud infrastructures such as O365, Azure, etc.). However, the most critical technology an effective MDR partner must provide is artificial intelligence. A proprietary AI platform woven throughout the full service will centralize and coordinate all detection and response activities, dramatically increasing their speed and accuracy.

White Paper

About Atos

Atos is a global leader in digital transformation with 110,000 employees and annual revenue of € 12 billion. European number one in cybersecurity, cloud and high performance computing, the group provides tailored end-to-end solutions for all industries in 73 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/ career

Atos Global Head Office
River Ouest, 80 quai Voltaire
95877 Bezons cedex – France
+33 1 73 26 00 00

Let's start a discussion together

For more information: **contact us now.**

CT-210105-AR-MDR-WP-Buyers-Guide-to-MDR-en-V2