Assessing MDR offerings - a handy guide

There are hundreds of MDR offerings out there, and it's important you choose a service that is right for your organization.

No two companies have the exact same needs, and there is no such thing as a perfect out-of-the-box solution. That means it's crucial that you can identify what is most important to you in terms of security and match those requirements to the MDR services on offer.

Before you dive into the detail of each service offering, we recommend identifying what is driving your need for increased security and what kind of risk profile you have. This information will seriously impact the kind of service you will need.

What is driving your security needs? - Legal requirements, e.g. NIS2 or ISO 270001? - Internal risk management policies? - Supply chain requirements?	What is your company's risk profile? Think about industry, customer base, data sensitivity, geopolitics, and whether you or similar companies have been targeted before.
Notes:	Notes:

Understand the offering

Use the following checklist to assess individual services by marking off everything they offer. When you understand your own priorities, you can highlight the aspects of a service that are most important to you.

Area	Specific offering	Tick
Compliance and Regulatory Support	**Compliance expertise**: Guidance on relevant regulations and standards	
	Compliance reporting: Regular reports that demonstrate adherence to required standards.	
	Audit support: Assistance preparing for and navigating compliance audits.	
Customization and Flexibility	**Tailored solutions**: Customizing the MDR service to fit the unique needs and risk profiles of each organization.	
	Scalability: The ability to adjust services as the organization grows or changes.	
	Service level agreements: Clearly defined expectations and performance metrics.	
Resource and Budget Alignment	**Cost transparency**: Clear and predictable pricing models.	
	Resource efficiency: Optimizing resource allocation to maximize effectiveness and minimize waste.	

Incident Detection and Response Capabilities	**Detection accuracy**: Technology that minimizes false positives and ensures real threats are identified promptly.	
	Response speed: Crucial for minimizing damage and disruption.	
	Proactive threat hunting: Active searches for potential threats that have not yet been detected by automated systems.	
	Breach response support: Immediate assistance in the event of a security breach, including containment, investigation, and remediation efforts.	
	24/7 monitoring: Continuous surveillance of the organization's network and systems to detect and respond to threats at any time.	
	Identity-related attack support: Expertise around managing attacks when one or more user accounts have been compromised.	
Technology and Integration	**Integration with existing systems**: Whether the MDR service can seamlessly integrate with the organization's current I T infrastructure.	
	Cloud and on-premises support: Flexibility to protect both cloud-based and on-premises environments.	
Reporting and Transparency	**Real-time reporting**: Immediate access to current threat data and security status.	
	Detailed reporting: Comprehensive reports that provide in-depth analysis of security events, trends, and system performance.	
	Incident reporting: Specific reports on individual security incidents, detailing the nature of the threat, the response taken, and lessons learned.	
Vendor Management and Supply Chain Security	**Third-party risk management**: Assessing and mitigating risks associated with third-party vendors and partners.	
	Supply chain visibility: Assessing and mitigating risks associated with organizations in the supply chain.	
Support and Expertise	**Cybersecurity expertise**: Access to a team of seasoned cybersecurity professionals who can offer expert advice and insights.	
	Training and awareness: Programs to educate staff on cybersecurity best practices.	
	Human support/escalation: Direct access to human experts for critical issues.	

Incident Preparedness	**Incident response playbooks**: Predefined strategies and procedures to follow in the event of security incidents.	
	Business continuity planning: Ensuring that the organization can continue operating when incidents occur.	
Continuous Improvement	**Threat intelligence updates**: Regular updates on emerging threats and vulnerabilities.	
	Service evolution: The ability to evolve and improve over time, incorporating new technologies and methodologies.	
	Client feedback loop: Mechanisms for gathering and acting on client feedback.	
References	**Client references**: Testimonials and references from current or past clients that demonstrate the effectiveness and reliability of the MDR service.	
	Case studies: Detailed examples of how the MDR service has successfully protected organizations in the past.	

If you've identified a few of the items above as high-priority, good news!

WithSecure MDR may be the perfect fit for your company, as everything on this checklist is included in our comprehensive service.

WithSecure's cyber security experts protect your IT environment by monitoring, investigating, and remediating cyber security attacks across your estate, so trust in our proven track record and get in touch to learn more.

Contact us