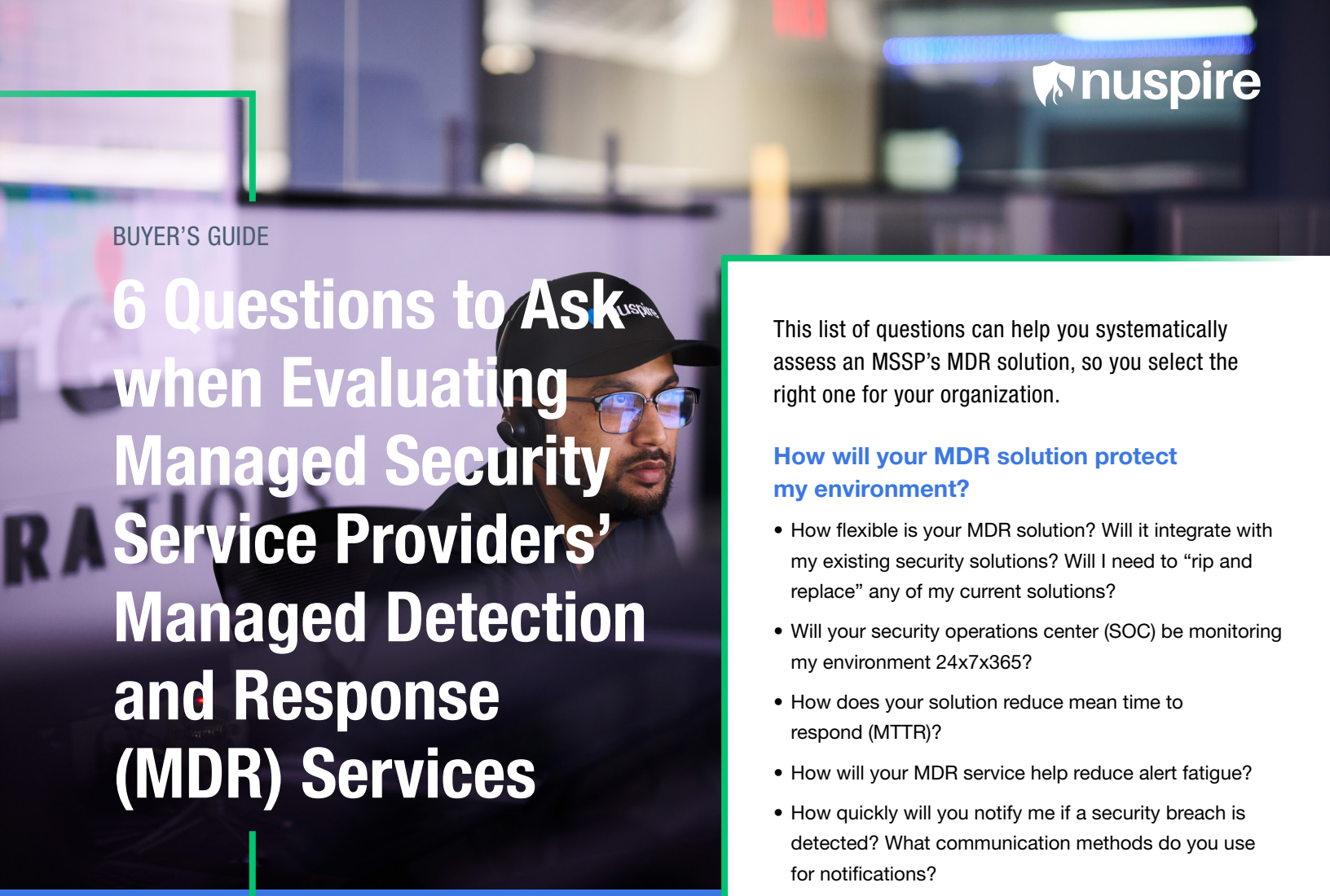

BUYER'S GUIDE

6 Questions to Ask when Evaluating Managed Security Service Providers' Managed Detection and Response (MDR) Services

Security professionals are experiencing alert fatigue and are looking for a solution that supports faster response times. Your team may also be struggling with managing multiple, disparate security tools and to provide 24x7x365 monitoring and triaging due to the IT security talent shortage.

Engaging a knowledgeable third-party, such as a managed security service provider (MSSP), can take the pressure off. Additionally, an MSSP with managed detection and response (MDR) technology can identify and respond to threats efficiently and quickly.

However, with hundreds of MSSPs to choose from, how do you know which one is a good fit for your organization? Not all MSSPs' MDR services are the same, so it's important to be thorough when you're evaluating potential providers.

This list of questions can help you systematically assess an MSSP's MDR solution, so you select the right one for your organization.

How will your MDR solution protect my environment?

- How flexible is your MDR solution? Will it integrate with my existing security solutions? Will I need to "rip and replace" any of my current solutions?
- Will your security operations center (SOC) be monitoring my environment 24x7x365?
- How does your solution reduce mean time to respond (MTTR)?
- How will your MDR service help reduce alert fatigue?
- How quickly will you notify me if a security breach is detected? What communication methods do you use for notifications?
- Will your platform let me view my entire security environment, including endpoint, network and cloud data, in a single consolidated dashboard?
- How will you customize your MDR service to support my environment such as supporting flexible vulnerability scans, security appliances, Wi-Fi and network edge management?
- What is your MDR service's balance between human intelligence and technology?
- Do you employ a Security Operations Center (SOC) with knowledgeable analysts with experience in incident investigation and response with threat containment? Do you operate a Tier 3 SOC?
- Do you have an incident response team that includes security intelligence and analytics experts; security incident team implementation experts; health, availability, lifecycle and optimization infrastructure and system experts and security and incident response team experts?
- Do you have an incident response team that can complement my in-house team's expertise?
- Do you support multiple security profiles?

- Will your service centralize monitoring and management of my environment? Will it eliminate maintaining multiple, disparate security tools?
- Can you prevent programs from being installed that violate our corporate policies?
- Do you support exclusions and blacklists?
- What security frameworks do you use? (MITRE ATT&CK, NIST, etc.)

What is your onboarding process?

- Do you have a formalized onboarding process that includes a deep discussion about risk, goals, industry and asset inventory? How often is this process repeated and updated?
- How long does it take to onboard a new client? Do you have a flexible and customized onboarding process? Will it include a customized runbook?
- Will the runbook outline when alerts should be taken seriously, escalation process and when suspicious activity should be flagged?
- What is your deployment process? Do you support command line installations?

What technologies does your MDR service support?

- Is your MDR platform technology-agnostic and does it support leading technologies?
- How does your MDR platform eliminate the need for multiple security tools?
- Does your MDR service use SIEM technology to correlate logs? Can it match alert data against predetermined security rules?
- Does your MDR service support Extended Detection and Response (XDR)?
- Does your MDR technology support: a portal; reporting; using multiple technology sources enriched with threat data, client data and the dark web; User Entity and Behavior Analytics (UEBA); inventorying and managing endpoints and rapid data ingestion?
- Do you support a centralized managed console that's hosted in the cloud?
- Can you identify gaps in my current security processes and determine where we need to maximize visibility in order to predict potential risk?
- How do you incorporate advanced tools like log management, security information and event management (SIEM), use case analytics, behavior analysis, business context and pattern discovery to detect and prioritize threats?
- What types of dashboards, log search, dynamic drill downs and reports do you offer?
- How will you continuously assess, monitor and improve my security posture?
- How do you correlate security events with threat intelligence to reduce false positives?
- Do you use analytics-based insights from global threat traffic? What types of intelligence data do you use?
- Do you have cross-platform visibility across my endpoints?
- What platforms do you support for user endpoint clients, server endpoint clients and virtual environments?

What is your process for finding potential threats and selecting actionable alerts to send us?

- Does your MDR service have any automations such as for threat hunting, alert enrichment or runbook prioritization?
- How do you sort out false positives from alerts that could be true threats?
- Do you support continuous visibility, security and compliance monitoring across public, multi-cloud deployments?
- Can you provide near real-time, customized alerting?
- Can you create rules to alert for incidents such as “1 GB of data is being exfiltrated”?
- If you find a threat, will you alert me, provide details of the response and tell me further actions I should take?
- Do you monitor traffic as it passes through your infrastructure, examine syslogs and perform API analysis?
- What is your process for mitigating and quarantining security events? How quickly can you mitigate and quarantine suspicious activity?
- Do you offer autonomous, multi-layered protection that covers all attack vectors – even when offline?
- Do you automatically initiate threat hunting when you detect a possible security incident?
- What criteria will you use to determine if a threat should be escalated?

How do you leverage threat intelligence?

- Does your intelligence team specialize in threat intelligence? Does it leverage data from multiple sources, correlate it and enrich the data?
- Does your MDR service pull in multiple sources of telemetry such as from my network, endpoint and cloud environments?
- Do you enrich security telemetry with third-party and your own threat intelligence such as identity and digital trust, email security and Internet of Things (IoT)?
- Does your solution support analysis of encrypted traffic?

Do you have happy, satisfied customers?

- What are your service level agreements (SLAs) for different events? What happens if you miss an SLA?
- What is your Net Promoter Score (NPS) and customer retention rate?
- Can we talk to some of your current customers about their experiences with your company?

nuspire