BUYER'S GUIDE

6 Questions to Use when Evaluating Managed Security Service Providers' Endpoint Detection and Response (EDR) Services

Endpoint detection and response (EDR) solutions give security professionals visibility into the cybersecurity posture of their company's endpoints such as laptops, desktops, mobile phones, Internet of Things (IoT) devices and more. However, EDR solutions often produce a huge volume of alerts, including false positives, which can result in alert fatigue. Many organizations also lack experienced security professionals to monitor and manage their EDR solutions.

Engaging a knowledgeable third-party, such as a managed security service provider (MSSP), can take the pressure off your IT team. Additionally, an MSSP has the technology in place to 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 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 EDR solution, so you select the right one for your organization.

How will your EDR solution protect my environment?

- How flexible is your EDR solution? Will it integrate with my existing security solutions? Will I need to "rip and replace" any of my current solutions?
- Do your solutions support real-time detection across all my endpoints?
- Do you employ a Security Operations Center (SOC) with knowledgeable analysts who have experience in incident investigation and response with threat containment? Do you operate a Tier 3 SOC?
- Will your security operations center (SOC) be monitoring my endpoints 24x7x365?
- How quickly will you notify me if a security breach is detected? What communication methods do you use for notifications?
- How long do you retain logs?
- Do you support multiple security profiles?
- Will your service centralize monitoring and management of my environment? Will it eliminate maintaining multiple, disparate security tools?
- Do you have cross-platform visibility across my endpoints?

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 EDR service support?

- Do you use machine learning technology to detect security events? Can your machine learning detect and prevent signature-less advanced malware?
- Does your solution support analysis of encrypted traffic?
- Do you deploy a lightweight agent?
- Do you support a centralized managed console that's hosted in the cloud?
- Do you offer a SIEM service? Can it match alert data against predetermined security rules?
- What platforms do you support for user endpoint clients, server endpoint clients and virtual environments?
- What security frameworks do you use? (MITRE ATT&CK, NIST, etc.)

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

- What is your process for mitigating and quarantining security events? How quickly can you mitigate and quarantine suspicious activity?
- Can you prevent programs from being installed that violate our corporate policies?
- Can you create rules to alert for incidents such as "1 GB of data is being exfiltrated"?
- Do you support exclusions and blacklists? Do you offer autonomous, multi-layered protection that covers all attack vectors – even when offline?

How do you leverage threat intelligence?

- How do you enrich alerts with threat intelligence?
- 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 correlate security events with threat intelligence to reduce false positives?
- Does your solution correlate telemetry from multiple data sources such as endpoints, cloud and networks?

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