vijilan
IT Security: Enabled

10 QUESTIONS TO ASK

BEFORE CHOOSING AN EDR PROVIDER

WHY THESE QUESTIONS MATTER

EDR (Endpoint Detection & Response) is your last line of defense when attackers reach endpoints. Not all EDR is created equal—these questions separate real protection from checkbox compliance.

THE QUESTIONS

1 What detection methodology do you use—signatures, behavioral, or both?

Why it matters: Signature-based detection misses novel threats. Behavioral detection (IOA) catches attacks that signatures can't.

What to look for:
- Indicators of Attack (IOA) behavioral detection
- Machine learning/AI components
- Signature detection as supplement
- Fileless malware detection

🚩 Red flag: Heavy reliance on signatures or "next-gen AV" marketing.

2 What's the agent footprint and performance impact?

Why it matters: Heavy agents slow endpoints and frustrate users. Some agents consume 5-10% CPU—unacceptable for production systems.

What to look for:
- < 1% CPU usage
- < 50 MB memory
- Single agent for all capabilities
- No full-disk scans

🚩 Red flag: Multiple agents required or "minimal impact" without specifics.

3 What response actions can you take remotely?

Why it matters: Detection without response is just an expensive alert system. True EDR enables immediate action.

What to look for:
- Network isolation
- Process kill/quarantine
- File deletion/quarantine
- Remote shell access
- Registry/startup cleanup

🚩 Red flag: "Alerts only—response is manual."

4 How do you handle cloud-native and container workloads?

Why it matters: Modern infrastructure includes containers and serverless. Traditional EDR doesn't protect these environments.

What to look for:
- Container runtime protection
- Kubernetes visibility
- Serverless monitoring
- Cloud workload protection included

🚩 Red flag: "Containers are a separate product" or not supported.

5 What visibility do you have into identity-based attacks?

Why it matters: Attackers increasingly use valid credentials. EDR alone can't see credential theft or lateral movement via authentication.

What to look for:
- Integration with identity protection
- Credential theft detection
- Lateral movement visibility
- Combined endpoint + identity correlation

🚩 Red flag: No identity capabilities or "that's a different tool."

6 Is managed detection and response available?

Why it matters: Even the best EDR generates alerts that need investigation. Managed services provide 24/7 expert coverage.

What to look for:
- 24/7 managed option
- Human analysts reviewing alerts
- Active response capabilities
- Clear SLAs

🚩 Red flag: "Self-service only" or managed services from third party.

7 How quickly can you deploy across our environment?

Why it matters: Lengthy deployments leave endpoints exposed. Modern EDR deploys in hours, not weeks.

What to look for:
- Mass deployment options (GPO, SCCM, Intune)
- 24-48 hour deployment possible
- No infrastructure prerequisites
- Cloud-native management console

🚩 Red flag: "Plan for 4-6 weeks" or on-prem server requirements.

8 What operating systems and versions are supported?

Why it matters: Legacy systems and diverse OS environments need coverage. Gaps leave attack vectors open.

**What to look for:
- Windows (including legacy versions)
- macOS (current and recent)
- Linux (major distributions)
- Mobile options available

🚩 Red flag: Limited OS support or recent versions only.

9 How does pricing scale with growth?

Why it matters: Some vendors penalize growth with steep per-endpoint costs. Understand pricing before you're locked in.

What to look for:
- Clear per-endpoint pricing
- Volume discounts available
- No hidden feature fees
- Predictable annual cost

🚩 Red flag: Opaque pricing or "contact sales for every quote."

10 What third-party validation exists?

Why it matters: Marketing claims are easy. Independent testing proves real-world effectiveness.

What to look for:
- Gartner Leader or Challenger
- Forrester Leader
- MITRE ATT&CK evaluation results
- SE Labs/AV-TEST results

🚩 Red flag: No third-party validation or cherry-picked metrics.

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN

EVALUATION SCORECARD

Question	Weight	Score (1-5)	Notes
Detection methodology	Critical		
Agent performance	High		
Response capabilities	Critical		
Cloud/container support	High		
Identity integration	High		
Managed services	Medium		
Deployment speed	Medium		
OS coverage	Medium		
Pricing model	Medium		
Third-party validation	High		
TOTAL		/50	

AICPA SOC

International Organization for Standardization ISO 27001

A-LIGN

HOW VIJILAN ANSWERS

Question	Vijilan Answer
Detection	IOA behavioral + AI/ML (Falcon)
Agent footprint	< 1% CPU, ~40 MB memory
Response actions	Full remote response capabilities
Cloud/containers	Falcon Cloud Security included
Identity	ITDR included in Premium
Managed	24/7 SOC with remediation
Deployment	24-48 hours
OS support	Windows, macOS, Linux
Pricing	Transparent per-endpoint
Validation	CrowdStrike: Gartner Leader

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988

SCAN HERE TO BOOK A FREE DEMO