vijilan
IT Security: Enabled

EDR VENDOR COMPARISON

ENDPOINT DETECTION & RESPONSE: CROWDSTRIKE VS. ALTERNATIVES

QUICK COMPARISON

Capability	CrowdStrike (Vijilan)	Microsoft Defender	SentinelOne	Carbon Black	Sophos
Detection	IOA + AI/ML	Signature + AI	AI/ML	Signature + Behavioral	Signature + AI
Agent Footprint	< 1% CPU	2–5% CPU	< 2% CPU	2–5% CPU	2–5% CPU
Cloud-Native	✓	✓	✓	Hybrid	Hybrid
Identity (ITDR)	Native	Separate (Defender for Identity)	Add-on	✗	✗
Gartner Ranking	Leader	Leader	Leader	Challenger	Niche
Managed Service	✓ (Vijilan)	Defender Experts	Vigilance	Varies	MTR

DETECTION METHODOLOGY

Platform	Primary Detection	Secondary Detection	Key Strength	Overall Result
CrowdStrike Falcon	Indicators of Attack (IOA) — behavioral detection	AI/ML, signatures for known threats	Catches fileless and living-off-the-land attacks	Highest efficacy in independent tests
Microsoft Defender for Endpoint	Signature-based + cloud AI	Behavioral analytics	Deep Microsoft ecosystem integration	Best for M365-heavy environments
SentinelOne	Autonomous AI	Behavioral detection + signatures	Strong automation and rollback capability	Good efficacy with advanced automation
VMware Carbon Black	Behavioral analytics	Signatures	Legacy presence and threat hunting	Solid but aging platform

vijilan
IT Security: Enabled
vijilan.com
info@vijilan.com
+1 (954) 334-9988

MANAGED EDR COMPARISON

Capability	Vijilan + CrowdStrike	Microsoft Defender Experts	SentinelOne Vigilance
24/7 Monitoring	✓	✓	✓
Full Remediation	✓	Limited	Limited
Response SLA	15 minutes	Best effort	30 minutes
Identity Protection	Included	Separate product	Add-on
Threat Hunting	Included	Included	Included
Deployment Support	✓	Limited	✓

AGENT PERFORMANCE

Metric	CrowdStrike	Microsoft Defender	SentinelOne	Carbon Black
CPU (Idle)	< 1%	2–3%	1–2%	2–4%
CPU (Active Scan)	1–2%	5–10%	2–4%	5–10%
Memory Usage	~40 MB	~100 MB	~50 MB	~80 MB
Disk Footprint	~50 MB	~200 MB	~100 MB	~150 MB

PLATFORM CAPABILITIES

Feature	CrowdStrike	Microsoft Defender	SentinelOne	Carbon Black
EDR / XDR	✓	✓	✓	✓
Identity (ITDR)	✓ Native	Separate product	Add-on	✗
Cloud Security	✓	✓	Limited	✗
Vulnerability Management	✓ Native	✓	Add-on	✗
Log Management	✓ (LogScale)	Sentinel (additional cost)	✗	✗
Threat Intelligence	✓ Premium	✓	✓	✓

vijilan
IT Security: Enabled
vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN

QUESTIONS TO ASK COMPETITORS

1. What's the real-world CPU impact?
2. Is identity protection native or a separate product?
3. What's included in the managed service vs. extra?
4. Show me your MITRE ATT&CK evaluation results.
5. What's the response SLA for your managed offering?

KEY DIFFERENTIATORS

Why CrowdStrike (via Vijilan) Wins

Detection Efficacy

Consistently highest in MITRE ATT&CK evaluations.

Single Agent

One agent for EDR, identity, cloud, exposureâ€”not multiple.

Lightest Footprint

< 1% CPU impact vs. 2-5% for competitors.

Native Identity

ITDR built-in, not bolted on separately.

Managed by Experts

Vijilan SOC adds 24/7 human expertise.

READY TO COMPARE?

Schedule a demo

vijilan
IT Security. Enabled.

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

AICPA SOC

International Organization for Standardization ISO 27001

A-LIGN