

SentinelOne vs CrowdStrike

EDR Battle Card · AE Deal-Cycle Edition · Generated May 10, 2026

CROWDSTRIKE SNAPSHOT

Founded	2011 · HQ Sunnyvale, CA
Public/Private	Public (NASDAQ: CRWD)
Headcount	11,169 employees · +13.2% YoY · +3.9% QoQ
Annual Revenue	\$4.57B (vs SentinelOne \$956M → they are ~4.8x our revenue)
Total Funding (pre-IPO)	\$481M raised across 6 rounds
Product Portfolio	15 products spanning EDR, XDR, SIEM, Cloud, Identity, Exposure, IoT, AI Sec
Primary Category	Endpoint Security · same as us
Momentum (CybersecTools)	79/100 · "Accelerating" tier (we are 67/100, "Steady" tier)

HEAD-TO-HEAD COMPARISON

Metric	SentinelOne (Us)	CrowdStrike (Them)	Edge
Founded	2013	2011	Even
Headcount	3,157	11,169	Them ↑ scale
Headcount Growth (QoQ)	+7.8%	+3.9%	Us ↑ momentum
Headcount Growth (YoY)	+10.1%	+13.2%	Them ↑ absolute
Annual Revenue	\$956M	\$4.57B	Them ↑ scale
Total Funding (pre-IPO)	\$696.5M	\$481M	Us ↑ capital base
Product Portfolio	9 products	15 products	Them ↑ breadth
Employee Reviews (Glassdoor)	4.4 / 5.0 (866 reviews)	3.8 / 5.0 (1,300 reviews)	Us ↑ culture
Reviews Trend (YoY)	Stable (no change)	↓ -0.4 yearly	Us ↑ trajectory
CEO Approval	88%	87%	Even
Senior Mgmt Score	4.1 / 5.0	3.5 / 5.0	Us ↑ leadership
Website Traffic (mo)	652K visits	2.32M visits	Them ↑ awareness
LinkedIn Followers	386,722	1,007,956	Them ↑ reach
Momentum Score	67/100 (Steady)	79/100 (Accelerating)	Them ↑ signal

Source: CybersecTools MCP (April 2026 enrichment). Revenue figures are reported annual; headcount via LinkedIn enrichment.

EDR PRODUCT COMPARISON

	SentinelOne Singularity Endpoint	CrowdStrike Endpoint Security
Category	EDR (Endpoint Detection & Response)	EDR (Endpoint Detection & Response)
Deployment	Cloud-native, single agent	Cloud-native, single sensor
Cost Model	Commercial	Commercial
Company-Size Fit	SMB · Mid-Market · Enterprise	SMB · Mid-Market · Enterprise
MCP Integrations Tracked	6 (not yet enriched)	2 (limited dataset)

Core EDR Capabilities (per CybersecTools tool catalog)

SentinelOne Singularity Endpoint	CrowdStrike Endpoint Security
On-device AI for autonomous malware prevention	AI-powered protection (cited 100% MITRE ATT&CK 2025 score)
Behavioral & static AI models for ransomware	CrowdStrike Signal self-learning AI for unknown threats
Storyline technology — automatic event correlation	IOA methodology for malware-free attacks
One-click response with full rollback (Windows)	Automated response with agentic AI to reduce MTTR
Identity-based attack detection built into endpoint	Cross-domain attack visibility via Falcon platform
Mobile device protection vs zero-day & phishing	Single sensor across all major OSes
Generative AI for natural-language threat hunting (Purple AI)	Charlotte AI for triage, investigation, response
Real-time alert correlation across endpoints + identities	10GB/day third-party log ingest via Falcon Next-Gen SIEM
Man-in-the-middle attack protection	Real-time threat intel from CrowdStrike adversary tracking
Unified lightweight agent: Windows / macOS / Linux	—

WHY WE WIN

1. Our people stay — theirs are leaving

Data: SentinelOne 4.4/5.0 vs CrowdStrike 3.8/5.0 on Glassdoor. Their score has dropped 0.4 points YoY across senior management (-0.3), culture (-0.3), career opportunities (-0.3). Ours is stable.

Talk track: "When you buy security, you buy a team. The people delivering my product trust the company that builds it. CrowdStrike's own employees rate their senior management 3.5 — and that score has been falling for a year. That shows up in churn, in support response, in the engineer who picks up your P1 ticket at 2 AM."

2. We grew faster this past quarter, on purpose

Data: SentinelOne hired +7.8% QoQ vs CrowdStrike +3.9%. They added 423 people last quarter against an 11K base; we added 228 against a 3K base. Our hiring rate is roughly 2x theirs.

Talk track: "They're bigger — sure. But we're building. CrowdStrike's quarterly growth slowed to 3.9% this past quarter. Ours is 7.8%. That's engineering velocity, support capacity, and roadmap that gets shipped."

3. Autonomous response with rollback — not just detection

Data: SentinelOne Singularity Endpoint includes one-click rollback for ransomware encryption. CrowdStrike's feature set per CybersecTools catalog emphasizes detection + response orchestration via Charlotte AI, but no native rollback.

Talk track: "When ransomware fires, CrowdStrike tells you it happened. We undo it. Storyline correlates the attack chain, and one-click rollback restores files — native to the agent, not a separate backup product. That's the difference between a 30-minute incident and a 30-day one."

4. We were built AI-native, not retrofitted

Data: SentinelOne ships on-device AI for autonomous prevention — the engine runs on the endpoint, even offline. CrowdStrike Charlotte AI is cloud-side agentic AI. Both work, but architectural difference matters when the cloud is unreachable.

Talk track: "What happens to your detection when the laptop is on a plane, or your VPN drops, or there's a regional cloud outage? Our AI runs on the device. Theirs lives in their cloud. Ask which model your security relies on — the answer matters when the network breaks."

5. Recent CrowdStrike CVE — and the July 2024 incident still echoes

Data: CVE-2026-40050: critical unauthenticated path-traversal in CrowdStrike LogScale (April 2026). Allows remote attackers to read arbitrary server files. Still fresh.

Talk track: "Two weeks ago CrowdStrike published an emergency advisory — a critical vulnerability in their LogScale product letting unauthenticated attackers read files from the server. When the security vendor itself is the attack vector, that's a board-level conversation. Worth asking: how was it disclosed? What's their CVE history look like next to ours?"

WHERE THEY'RE STRONG (HANDLE WITH CARE)

■ Scale and revenue — 4.8x larger by revenue

Reality: CrowdStrike \$4.57B annual revenue vs SentinelOne \$956M. 11.2K employees vs our 3.2K. Wall Street loves them.

Reframe: *Acknowledge the number. Then pivot: scale is the past; trajectory is the future. We grew QoQ 7.8% to their 3.9%. The bigger they get, the slower they move on roadmap. The question isn't who's biggest — it's whose architecture wins the next five years.*

■ Broader product portfolio — 15 products vs our 9

Reality: CrowdStrike Falcon spans EDR, XDR, SIEM, Cloud, Identity, Exposure Mgmt, Data Protection, IoT/OT, AI Security. That's a real consolidation story for a CISO trying to retire 10 tools.

Reframe: *"They have more SKUs — we have a focused platform. If you want to consolidate every security category to one vendor, that's a CrowdStrike conversation. If you want best-in-class endpoint with deep autonomous response and identity — that's us. Most enterprises buy best-of-breed for the agent and integrate, because lock-in to one stack is a board risk."*

■ Brand awareness and analyst presence

Reality: 2.32M monthly website visits vs ours 652K. 1M LinkedIn followers vs 387K. Momentum score 79 (Accelerating) vs 67 (Steady).

Reframe: *Don't fight the brand on equal turf. Lean into "the buyer's shortlist always includes the obvious name — the question is what you find when you actually evaluate." Push for the POC. We win head-to-head bake-offs because the agent and the rollback are tangible. Analyst momentum doesn't survive a side-by-side technical eval.*

OBJECTION HANDLING

Objection: "CrowdStrike is the market leader — nobody gets fired for buying them."

Response: *Reframe: "That was true two years ago. The July 2024 outage took down hospitals, airlines, and 911 centers — nobody is using 'safe choice' to describe CrowdStrike anymore. Boards now ask why you didn't diversify. We're the credible #2 with stronger employee trajectory (4.4 vs 3.8 Glassdoor) and a different architecture — that's now a feature, not a risk."*

Objection: "We hear SentinelOne's CFO just left and revenue guidance was light."

Response: *Acknowledge directly: "Yes, our CFO transitioned in December. Q3 FY2026 revenue still grew 23% YoY — our growth rate is healthy and we have \$696M in pre-IPO funding plus public-market access. We're not slowing investment in the product. Compare to CrowdStrike's post-July-2024 trajectory — the question isn't executive transitions, it's engineering momentum, and ours is up 7.8% QoQ in headcount."*

Objection: "CrowdStrike has more products — we want one vendor for everything."

Response: *"Single-vendor strategies are great until they break, and when CrowdStrike broke last year it broke 8.5 million machines at once. Best-of-breed endpoint with strong integrations is the safer architecture. Singularity covers EDR, XDR, identity, and cloud — the categories that matter for endpoint protection. The other categories CrowdStrike sells (DLP, IoT, etc.) you can buy from specialists who do them better."*

Objection: "Their MITRE ATT&CK; 2025 results were 100%. Yours weren't cited."

Response: *"Both vendors do well in MITRE evaluations — SentinelOne has hit 100% detection in multiple recent rounds too. Press the prospect on what they actually want to test. Detection coverage is one axis. Time-to-respond, autonomy, false-positive rate, agent footprint, and rollback success rate matter more in a real environment. I'll set up a head-to-head POC — let the agents run side by side on your endpoints for 30 days."*

Objection: "CrowdStrike has Charlotte AI — isn't agentic AI the future?"

Response: *"Agentic SOC AI is exactly where the industry is going — and we ship Purple AI, our agentic platform, in the same Singularity console. Both vendors are racing here. The question is architecture: ours runs autonomous decisions on the device; theirs orchestrates from the cloud. When you're a CISO, the safer bet is the agent that still works when the network doesn't."*

QUICK DISMISS (ONE-LINERS)

- **On size:** "CrowdStrike is bigger — we grew headcount twice as fast last quarter. Bigger and slower is still slower."
- **On the outage:** "Boards used to ask 'why aren't we on CrowdStrike?' — now they ask 'what's our backup plan if CrowdStrike fails again?' We're the answer to question #2."
- **On AI:** "Their AI is in the cloud. Ours runs on the endpoint. Different architecture, different failure mode — ours doesn't go dark when the cloud does."
- **On rollback:** "When ransomware fires, CrowdStrike tells you. We undo it."

RECENT MOVES (LAST 30 DAYS)

CrowdStrike

- Apr 22, 2026 — **CVE-2026-40050:** critical unauth path-traversal in LogScale, allowing remote read of arbitrary server files. (*weaponize this*)
- Apr 23, 2026 — Launched Project QuiltWorks AI security coalition with OpenAI, Anthropic, Accenture, IBM, Kroll. (*positive PR — expect prospects to bring this up*)
- Dec 2025 — Beat Q3 FY2026 forecasts, stock rose; introduced real-time cloud detection & response.

SentinelOne

- Dec 4, 2025 — **Q3 FY2026 results:** revenue +23% YoY, ARR +23% YoY. Strong quarter.
- Dec 7, 2025 — CFO Barbara Larson announced departure; reduced revenue guidance — stock dropped 14%. (*prospect may bring up; have the response ready*)
- Dec 11, 2025 — CEO Tomer Weingarten sold ~\$1.89M in shares (planned 10b5-1 disposition).

All metrics from CybersecTools MCP · Last enriched April 2026 · Glassdoor data is publicly self-reported · Cite specific data points only when prospect is technical — generic talk tracks land better in early-stage conversations.