PRODUCTBEACON

ProductBeacon — State of Cyber Security Markets 2026, Front 5: The SOC Platform War

Yohay Etsion

Managing Director, ProductBeacon

2026-06-21

Disclosure: *This is ProductBeacon's independent, impartial market research, based solely on publicly verifiable signals, published on the open web. No vendor sponsors, no paywalled data, no analyst-firm reuse. It reflects ProductBeacon's independent view and is not investment advice. Full independence and sourcing methodology: Methodology →.*

By Yohay Etsion · Head of Product (Fractional), AXIA · Creator of Product Org OS · Author of Leading the Charge (2023) and Vision to Value (coming 2026)

AXIA is an AI-powered data-security (Insider Risk Management / DLP) company.

5.1 The Playing Ground

The Detection & Response segment is where an organization watches its own systems for signs of compromise and acts on what it sees. Three product categories make it up. **Endpoint Detection and Response (EDR)** instruments laptops, servers, and workloads to record process behavior and detect attacker activity on the device itself.[1] **Extended Detection and Response (XDR)** widens that lens beyond the endpoint, correlating signals from email, identity, network, and cloud into a single detection.[2] **Security Information and Event Management (SIEM)** ingests logs and events from the entire estate, stores them, and runs correlation and analytics to surface threats and satisfy retention requirements.[3]

The strategic story of 2026 is the collapse of these three into one buying conversation: a unified **"next-generation SOC"** platform that promises detection, investigation, and response on a single data and workflow plane.[4]

What this segment is *not* matters as much as what it is. It is not vulnerability management — finding unpatched software before an attacker does is a prevention discipline, not a detection one. It is not pure network detection and response (NDR), though SOC platforms increasingly consume NDR signals. And it is not data-security or DLP: the SOC platform asks "is something attacking us right now?", not "is sensitive data leaving the building?" Those are adjacent fronts, each with its own core question.

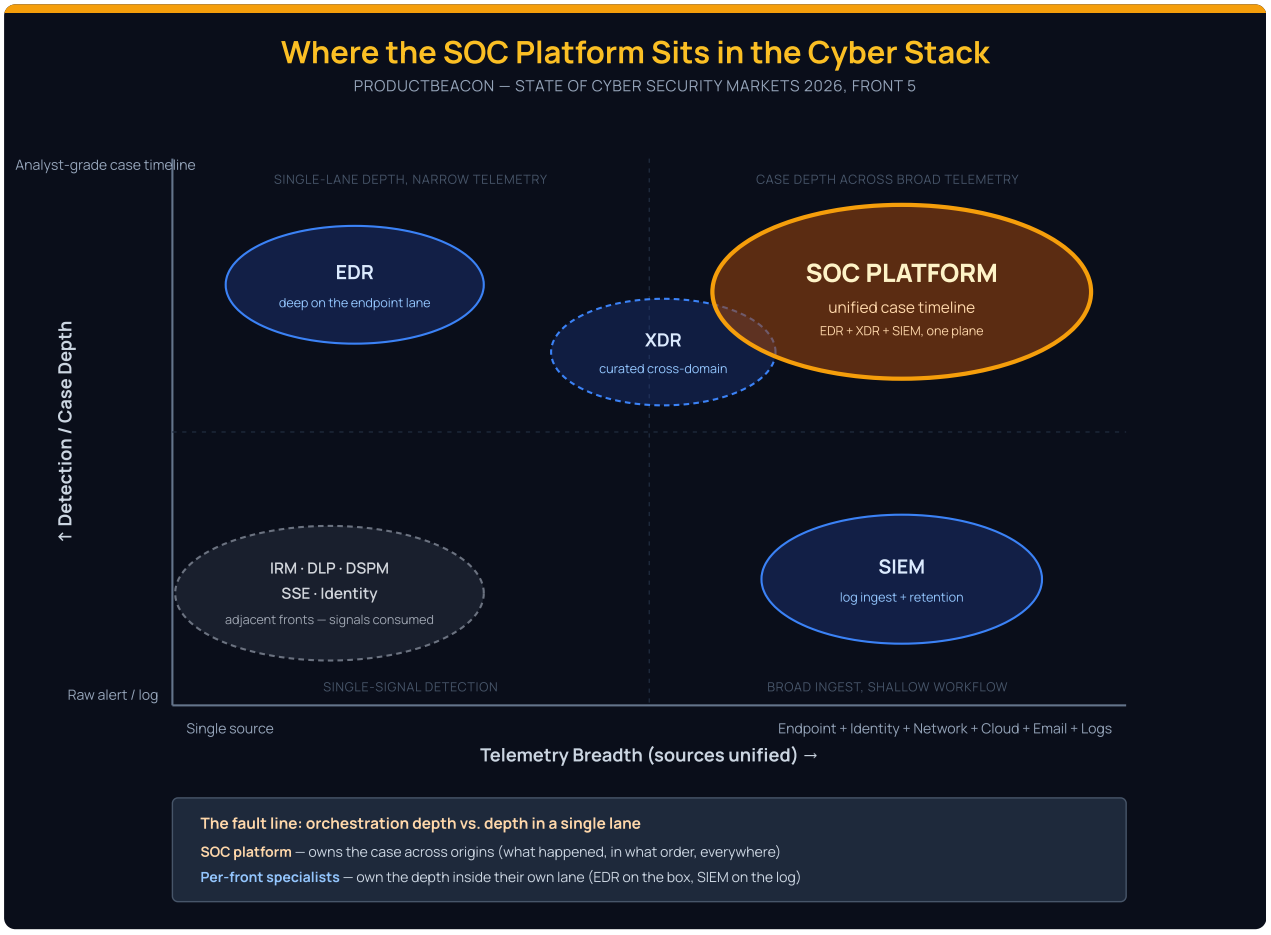
The shared foundation. The SOC platform's defining primitive is the **unified case timeline** — the single chronology of what happened, in what order, across every system, that an analyst works from end to end. As the report's taxonomy frames it, EDR/XDR/SIEM platforms increasingly *consume* signals from other fronts: Insider Risk Management, DLP, Data Security Posture Management, Secure Service Edge, and Identity. They then present a unified case workflow over all of them.[5] The same incident can originate as an insider exfiltration (IRM), a blocked transfer (DLP), an over-privileged access path (DSPM), an anomalous egress (SSE), or a privilege escalation (Identity). The SOC platform owns the orchestration of the case across those origins; the per-front platforms own the depth in their own lane. I read this division — orchestration depth versus depth in a single lane — as the fault line that decides who wins the best-of-breed-versus-platform argument. I return to it throughout this chapter.

Three buyer misconceptions are worth retiring before we map the market. The first is that **"XDR replaces SIEM."** It does not, cleanly. XDR correlates a curated set of high-fidelity sources well. But the compliance-grade log retention and arbitrary-source ingestion that SIEM provides remain a distinct requirement, which is precisely why the platform leaders are building data lakes underneath their XDR rather than retiring the SIEM tier.[4]

The second is that **"more telemetry means better detection."** Volume without curation raises both cost and analyst noise. The analyst-facing metric is signal quality, not gigabytes ingested, and the entire repricing tension described below flows from telemetry volume being a cost driver rather than a value

driver.[6]

The third is that **“the SIEM is just a log store.”** Treating it as passive storage misses where the product value — and the vendor lock-in — actually live: in the correlation, the detection-engineering, and increasingly the AI-investigation layer riding on top.[7]



The vertical axis is how deeply a platform reasons over a single data type; the horizontal axis is how many telemetry sources it unifies. SOC platforms claim the upper-right — broad ingestion plus a case timeline deep enough for an analyst to work — while per-front specialists hold the depth corners in their own lanes.

5.2 The Terrain

Market sizing — three lenses, deliberately not averaged. There is no single “SOC platform” number, because the segment is an aggregation of overlapping categories that analysts size separately. Read three lenses side by side rather than collapsing them.

On the **endpoint** lens, the EDR market is estimated at roughly USD 6.3 billion in 2026, projected to near USD 18.7 billion by 2031 at about a 24% CAGR. A broader Endpoint Protection Platform framing runs higher, around USD 7.2 billion for 2026.[8] On the **SIEM** lens, 2026 estimates cluster between roughly USD 8.4 billion and USD 12 billion, depending on whether managed services are folded in. Marketsandmarkets

puts the core SIEM market at USD 8.39 billion in 2026, growing to USD 13.67 billion by 2031 (~10% CAGR); Mordor Intelligence sizes it at USD 12.06 billion.[9] On the **XDR** lens, the youngest and most contested category, 2026 estimates range widely — from roughly USD 2 billion to USD 2.6 billion in conservative framings, up to high-single-digit-billions in aggressive ones, with growth rates above 20% on every estimate.[10]

The honest summary: the SIEM line grows in the low teens, while the EDR and XDR lines grow two to three times as fast. The gap between those growth rates is itself the market story — spend is migrating from passive log retention toward active, correlated detection.

Buyer trends. The dominant procurement shift is consolidation. Buyers who once assembled best-of-breed EDR, SIEM, and SOAR from separate vendors are increasingly evaluating a single platform that does all three, motivated by tool-sprawl fatigue, the cost of integration engineering, and the promise of one analyst workflow.[11] This is not universal — regulated enterprises with heavy compliance-retention obligations still keep a dedicated SIEM — but the center of gravity in mid-market and growth-stage buying has moved decisively toward the platform pitch. A second buyer trend is the rise of managed and co-managed operations: the SOC-as-a-service and MDR adjacencies are growing because the analyst-talent shortage makes a fully self-run SOC impractical for most organizations.[12]

Technology trends. Three are reshaping the segment. The first, and loudest in 2026, is the **agentic SOC analyst** — AI that does not merely surface alerts but autonomously gathers cross-stack evidence, builds attack timelines, and proposes or executes remediation. SentinelOne's Purple AI is the clearest production example: the company reported Purple AI attached to over half of all licenses sold in its fourth fiscal quarter. SentinelOne shipped one-click agentic Auto-Investigation at general availability while keeping an analyst-in-the-loop governance model.[13] Smaller entrants such as Dropzone AI push the same thesis from the autonomous-analyst edge.[14]

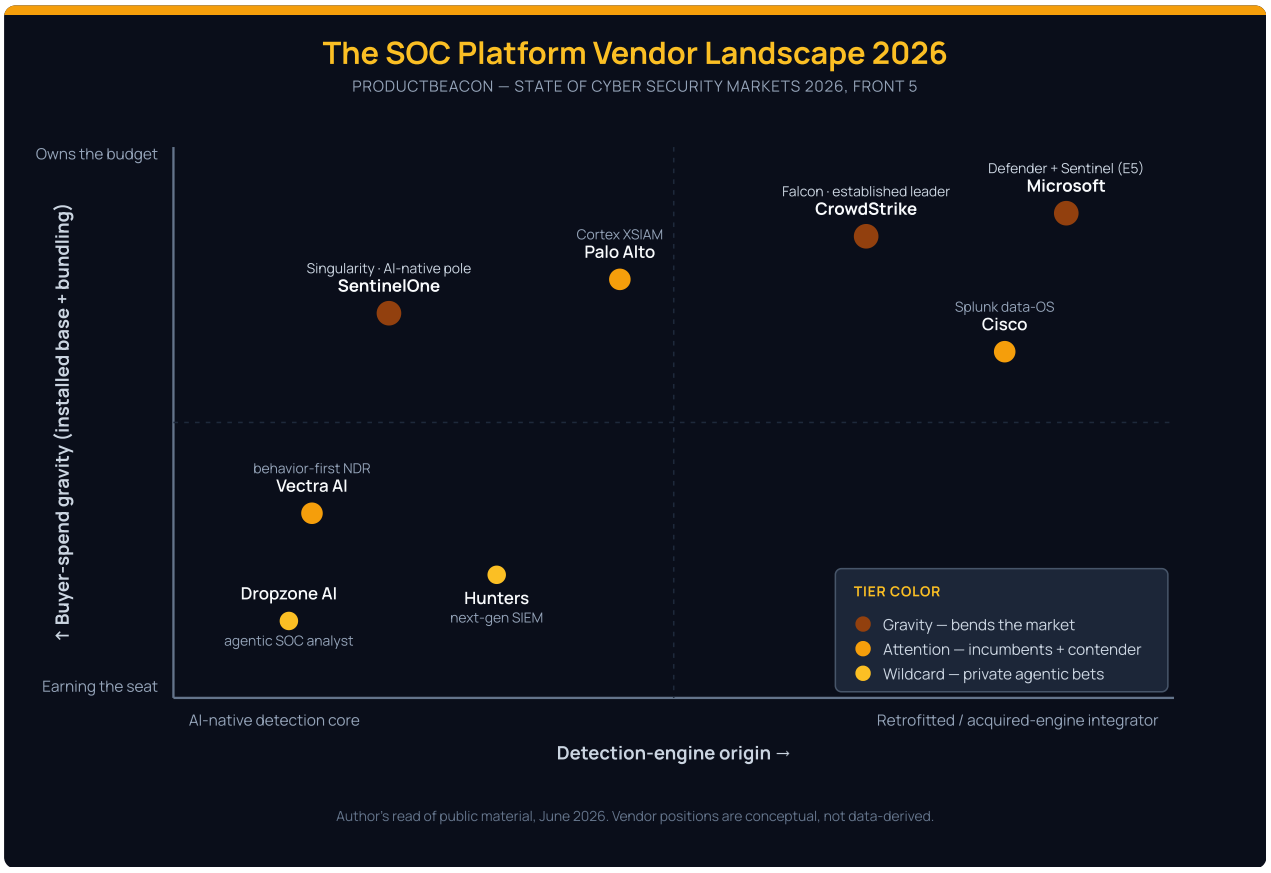
The second trend is **data-lake architecture**: rather than pay SIEM-tier prices to retain every log, platforms are splitting hot analytics from cheap long-term lake storage. Microsoft's Sentinel data lake is the reference implementation, with lake-only ingestion for Defender advanced-hunting tables now generally available. It sits under a Defender portal that Microsoft is positioning as the single SOC plane with embedded Security Copilot agents.[15]

The third trend follows directly: **telemetry-cost pressure is repricing the SIEM.** Because ingestion volume drives SIEM cost but not detection value in proportion, the vendors that can decouple the two gain pricing power, and those who cannot face margin compression. Cisco's Splunk-as-data-platform thesis is the largest bet here.[16] One currency note worth fixing: Microsoft's retirement of the Sentinel experience in Azure in favor of the Defender portal is scheduled for **2027-03-31**, not mid-2026. Any earlier date is out of date.[17]

Regulatory trends. The regulatory driver most specific to this segment is mandatory incident disclosure. In the United States, the SEC's rules require public companies to disclose a material cybersecurity incident on Form 8-K (Item 1.05) within four business days of determining the incident is material — a clock tied to the materiality determination, not the moment of discovery.[18] I read this as a structural tailwind for the SOC platform pitch. A four-business-day disclosure obligation makes fast, defensible detection-and-investigation a board-level requirement rather than a security-team preference, and the

platforms that can compress mean-time-to-understand are selling directly into that pressure. Government EDR mandates compound the effect: U.S. federal civilian agencies have been under binding deployment requirements that extended into cloud and identity coverage, pulling the public sector onto modern detection platforms on a regulatory timetable.[8]

5.3 The Contenders



Author's read of public material, June 2026. Vendor positions are conceptual, not data-derived.

The SOC platform field divides cleanly along two questions: who already owns the buyer's spend, and whether the detection engine was built AI-native or retrofitted onto a signature-and-correlation core. The eight vendors below are grouped into three tiers — Gravity (the three platforms that bend the market around them), Attention (the consolidating incumbents and the analytical contender flanking the leaders), and Wildcard (two private agentic-SOC bets characterized descriptively only). Each card is anchored to a single dated vendor-controlled surface and at least one verbatim messaging pillar.

Gravity tier

CrowdStrike

> *"The Agentic Security Platform. Unified and built to secure the AI revolution."* — [crowdstrike.com/en-us/platform, accessed 2026-06-16][19]

CrowdStrike is the category-defining endpoint platform. Its public messaging in mid-2026 has shifted from the long-running "we stop breaches" frame to an agentic-platform frame. The Falcon hero now reads as "the AI era is transforming cybersecurity across three critical fronts, and the CrowdStrike Falcon Platform secures them all."[20] The stated USP is unification around a single agent and single console: endpoint detection and response as the anchor, expanding outward into SIEM (Falcon Next-Gen SIEM, built on the LogScale logging engine) and identity. The target buyer is the enterprise SOC standardizing on one platform to retire a tool sprawl. Falcon's module-based pricing rewards that bundling: the more modules a customer lights up, the lower the per-module cost, and that discount is the commercial mechanism behind the platform pitch.

Architecturally, CrowdStrike classifies as cloud-native (the Falcon sensor reports to a cloud analytics backbone) and platform-over-best-of-breed. But it is fundamentally an *established-leader* posture: the detection core predates the current AI-native wave, and the agentic layer is being added on top of an established EDR engine. That established-leader framing is central to the front. It is the pole against which the AI-native challenger narrative (SentinelOne, below) defines itself.

The published-material tier here is the strongest in the front. George Kurtz remains chairman and CEO, and the company reported roughly $4.5 billion in cash and equivalents in its fiscal Q1 2026 filing. Its continued tuck-in acquisitions (including a January 2026 identity move) are documented in SEC filings and named-outlet coverage rather than vendor blog posts alone.[21] My read: CrowdStrike is the gravity well of this front, the vendor whose pricing and packaging choices set the reference point every other contender prices against.

Microsoft

> *"Prevent and disrupt threats with AI-powered, coordinated defense."* — [Microsoft Defender, microsoft.com/en-us/security/business/microsoft-defender, accessed 2026-06-16][22]
>
> *"Power your agentic defense with unified data and context."* — [Microsoft Sentinel, microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel, accessed 2026-06-16][23]

Microsoft's claim on this front rests on two products, not one: Defender for Endpoint as the EDR/XDR layer and Microsoft Sentinel as the cloud-native SIEM, with the Defender portal positioned as the single SOC plane that unifies both. Microsoft describes Sentinel as a "cloud-native SIEM that unifies AI, SOAR, UEBA, and TI," now wrapped in a unified data lake and "intelligent reasoning tools." It pairs the SIEM with Security Copilot agents for investigation.[24]

The stated USP is not a better detection engine — it is that the platform is *already there*: the buyer who runs Microsoft 365 E5 finds Defender and Sentinel inside a license they already pay for. That is the front's central platform-bundling story, and it is a pricing-pressure story before it is a capability story. E5 bundling compresses the standalone-EDR and standalone-SIEM deal that CrowdStrike, SentinelOne, and the independent SIEM vendors would otherwise win. The target buyer is the Microsoft-standardized enterprise; the architectural classification is cloud-native and platform-over-best-of-breed, with the SOC console (the Defender portal) as the unification surface.

One dated signal matters for currency: Microsoft extended the retirement of the legacy Sentinel-in-Azure experience to 2027-03-31, pushing the full migration into the Defender portal back from its earlier 2026 target.[25] The published-material tier is named-outlet plus vendor-controlled, and SEC-grade for the financials behind it (MSFT, NASDAQ). My read: Microsoft does not need to win on detection sophistication to reshape this front. Bundling does the work, and the platform-pressure thesis below is built on exactly that mechanism.

SentinelOne

> *"AI-native security powered by Autonomous Security Intelligence. See further. Stop faster. Gain the edge."* — [sentinelone.com, accessed 2026-06-16][26]

SentinelOne is the public-market pure-play that has staked the AI-native position most explicitly. Its homepage leads with "Built to Secure. Engineered for Advantage." and an "AI-native security powered by Autonomous Security Intelligence" pillar — language deliberately drawn to contrast with the established EDR engines.[26] The stated USP is autonomy: the Singularity platform and Purple AI "Auto-Investigations" frame the product as detection-and-response that runs at machine speed with less human triage.

The detail that matters most for classification, and the one a dated read would miss, is that SentinelOne is no longer accurately described as endpoint-pure. As of its fiscal Q1 2027 reporting (period ended 2026-04-30) the company disclosed roughly $1,163 million in ARR, up about 23% year over year. Roughly half of that ARR now comes from non-endpoint products — data, AI, and cloud.[27] The repositioning was reinforced by two September 2025 acquisitions, Prompt Security and Observo, both AI-pipeline and AI-security tuck-ins.[28]

The target buyer is the SOC that wants an AI-first platform without defaulting to the established leader; the architecture is genuinely AI-native and cloud-native, classified as platform rather than best-of-breed. Published-material tier is the strongest available — public reporter (S, NYSE), with ARR and acquisition figures from SEC filings and named-outlet coverage. My read: labeling SentinelOne "EDR" in 2026 understates it. It has become the cleanest articulation of the AI-native pole, which is precisely why the AI-native-versus-incumbent line is the front's central pattern claim.

Attention tier

Palo Alto Networks

> *"Unparalleled data. Unbeatable AI. The most advanced SOC platform."* — [Cortex XSIAM, paloaltonetworks.com/cortex/cortex-xsiam, accessed 2026-06-16][29]

Palo Alto Networks competes here through Cortex — Cortex XDR and, as the leading edge of its platform-expansion push, Cortex XSIAM, which the company markets as the place to "unlock true AI-driven security operations" and "the autonomous SOC built to stop tomorrow's threats."[30] The stated USP is convergence: XSIAM folds XDR, SOAR, and SIEM into one engine and pitches the SOC team on retiring the legacy SIEM entirely. The target buyer is the large enterprise consolidating a multi-tool SOC stack onto a single next-gen platform; the architecture classifies as AI-native at the analytics layer and platform-over-best-of-breed by design.

What earns Palo Alto its Attention-tier placement is not the SOC product alone but the capital behind it. The company recently closed two of the largest deals in the sector's history: CyberArk for roughly $25 billion (pulling identity security into the core platform; closed 2026-02-11) and Chronosphere for roughly $3.35 billion (cloud-native observability for AI-era data; closed January 2026). Cortex AgentiX is being integrated against Chronosphere for agentic find-and-fix.[31] That makes Palo Alto the most aggressive acquirer in the set, and its war chest the largest signal in the table below.

Published-material tier is named-outlet plus SEC-grade (PANW, NASDAQ). My read: Cortex/XSIAM is a credible next-gen SOC contender on its own, but Palo Alto's real advantage on this front is the acquisition engine — it is buying its way across identity, observability, and detection faster than any rival can build.

Cisco

> *"Tired of disconnected tools? Meet the new standard for threat detection, investigation, and response (TDIR)."* — [Splunk Enterprise Security (a Cisco company), splunk.com/en_us/products/enterprise-security.html, accessed 2026-06-16][32]

Cisco's claim on the SOC runs through Splunk, the $28 billion acquisition that closed in 2024 and reshaped the SIEM landscape.[33] The Splunk Enterprise Security product page — now footed as a Cisco company — positions the product as "a unified TDIR platform, seamlessly integrated with agentic AI, SOAR, UEBA, and SIEM." Cisco wraps Splunk's data engine together with Cisco XDR, Hypershield, and AI Defense into a single security narrative.[34] The stated USP is the data operating system: Splunk's ingestion and analytics layer as the system of record for the SOC, with Cisco's network telemetry and threat intelligence (Talos) feeding it.

The target buyer is the large enterprise already running Splunk or Cisco networking that wants the SIEM and detection layer bundled with infrastructure it owns — the same cross-sell pricing-power play Microsoft runs, but anchored on networking rather than productivity. Architecturally Cisco is a hybrid, a platform-over-best-of-breed integrator stitching acquired engines together rather than a single AI-

native core. The open question this front returns to in §5.6 is whether that integration can credibly replace a best-of-breed SIEM. Cisco reported roughly $1.95 billion in quarterly security revenue (up about 9% year over year) and reportedly around 5,000 customers across its newer security products.[35]

Published-material tier is named-outlet plus SEC-grade (CSCO, NASDAQ). My read: Cisco's Splunk integration is the bellwether for whether platform bundling can swallow the SIEM category — if it works, best-of-breed SIEM contracts; if it stalls, the independents get a reprieve.

Vectra AI

> *"AI-native, not AI nonsense."* — [vectra.ai, accessed 2026-06-16][36]

Vectra AI is the analytical contender of the Attention tier — the private specialist whose differentiation thesis is behavior-first detection rather than signature or correlation. Its homepage frames the pitch bluntly as "AI-native, not AI nonsense" and "we protect modern networks from modern attacks, Vectra AI sees attackers' every move, connecting the dots across network, identity, and cloud."[36] The stated USP is Attack Signal Intelligence: detection driven by attacker behavior across network, identity, and cloud, positioned against the alert-noise problem that the established correlation engines generate. The target buyer is the SOC that wants high-fidelity detection layered over (not replacing) its existing SIEM — an analytical complement more than a platform play. Vectra's 2026 acquisition of Netography nudges it toward converged cloud observability. The architecture is AI-native and best-of-breed by positioning rather than platform integrator.

Two facts correct any "challenger" framing. Vectra was named a Leader in the 2026 Gartner Magic Quadrant for Network Detection and Response for the second consecutive year, and it is a private unicorn valued at roughly $1.2 billion, having raised roughly $425 million across its history.[37] Published-material tier is named-outlet (analyst coverage, funding announcements) plus vendor-controlled. My read: Vectra is the clearest case in the front that "best-of-breed AI detection" still commands an analyst-validated seat at the table even as the platforms consolidate around it. But it is the smallest and least bundled of the public-facing contenders, which is its structural vulnerability if the consolidation thesis holds.

Wildcard tier

Hunters

> *"AI-Driven Next-Gen SIEM. Automated detection, investigation & response for small SecOps teams."* — [hunters.security, accessed 2026-06-16][38]

Hunters is the Israeli SOC platform that positions itself as a SIEM replacement. It leads with "AI-Driven Next-Gen SIEM" and the buyer-side promise of "a SIEM that works for you, not the other way around."[38] Descriptively, the stated USP is built-in detection engineering and automated investigation delivered as a platform rather than a toolkit the customer must assemble — aimed at SOC teams that want SIEM

outcomes without the operational overhead the legacy SIEM imposes. The target buyer described on its surfaces skews toward leaner SecOps teams. Architecturally it presents as cloud-native and SIEM-replacement in framing. On the funding picture, the most recent verifiable round is the $68 million Series C from January 2022 (roughly $118 million raised in total). No newer raise surfaced in the bounded scan, so this card makes no claim of recent capital.[39] Published-material tier is vendor-controlled plus the 2022 named-outlet funding coverage. I keep this read descriptive, and Hunters does not feature in the pattern claims that close this chapter.

Dropzone AI

> *"Reinforce your SOC with AI Analysts. Hunt, investigate, and respond at machine scale."* — [dropzone.ai, accessed 2026-06-16][40]

Dropzone AI is the agentic-SOC-analyst wildcard — the smallest-vendor edge of the AI-native SecOps story. Its homepage describes an "Agentic SOC" that "continuously adapts your detection and response," with an "AI SOC analyst" that "replicates the techniques of elite analysts to autonomously investigate and solve every alert."[40] Descriptively, the stated USP is autonomous alert investigation: an AI analyst that triages and investigates Tier-1 alerts without a human in the loop, sold to SOC teams drowning in alert volume. The target buyer described on its surfaces is the resource-constrained or alert-saturated SOC looking to offload investigation labor. Architecturally it presents as agentic and AI-native by construction rather than retrofit. On funding and scope, Dropzone raised a $37 million Series B in July 2025 led by Theory Ventures, and reports more than 100 customers. It has signaled an expansion from triage into full-spectrum detection, with an AI Threat Hunter and AI Threat Intel Analyst slated for the first half of 2026.[41] Published-material tier is vendor-controlled plus named-outlet funding coverage. I keep this read descriptive, and Dropzone does not feature in the pattern claims that close this chapter; the agentic-SOC thesis it embodies is examined in depth in the AI Security front (Front 7).

5.4 Their Plays

The SOC platform market is not fighting over features in 2026. It is fighting over what counts as the platform. Four plays are in motion, and each one is an argument about where the gravity of the security operations center should sit: in the detection engine, in the data layer, in the AI analyst, or out at the edge. Below, each play is stated as an observation grounded in a public signal, the named participants, and a conditional outcome that resolves against something an outsider can actually watch happen.

Play 1: The Next-Gen-SOC Consolidation Play

- **Observation.** Palo Alto Networks closed two of the largest security acquisitions of the cycle weeks apart: CyberArk for roughly $25 billion (completed 2026-02-11) and Chronosphere for roughly $3.35 billion (completed January 2026).[42] The stated logic is to fold identity security and cloud-native observability directly into the Cortex platform, with Cortex AgentiX wired to Chronosphere telemetry for agentic find-and-fix.[43] In parallel, Cortex XSIAM passed $500 million in ARR, with more than 600

customers and an average ARR near $1 million per customer, per the company's fiscal Q2 2026 earnings.[44]

- **Participants.** Palo Alto Networks (Cortex XSIAM, AgentiX, post-CyberArk identity, post-Chronosphere observability); cross-front overlap with the identity consolidation analyzed in Front 8.
- **Conditional outcome.** *If Palo Alto's next two fiscal quarters report XSIAM ARR continuing past the $500 million mark, with identity and observability cited as attach drivers on the earnings call, we expect the "next-gen SOC as one platform" thesis to harden into a named analyst category. If instead XSIAM ARR growth decelerates, or the CyberArk and Chronosphere integrations slip out of the earnings narrative, the deal-making reads as financial engineering rather than a platform reordering.*
- **Evidence.** Palo Alto Networks press release, Chronosphere completion, 2026 (paloaltonetworks.com, accessed 2026-06-16); Verdict, CyberArk deal, 2026 (verdict.co.uk, accessed 2026-06-16); Palo Alto Networks fiscal Q2 2026 earnings coverage, February 2026 (accessed 2026-06-16).

Play 2: The Splunk-as-Data-OS Play

- **Observation.** Cisco continues to integrate Splunk, acquired for roughly $28 billion and closed in 2024, as the data operating system underneath its security portfolio. That integration makes ThousandEyes, Hypershield, AI Defense, and AppDynamics first-class Splunk telemetry sources.[45] Cisco's security revenue runs near $1.95 billion per quarter, and its newer security products reportedly span roughly 5,000 cumulative customers.[46] The bet is that owning the telemetry layer lets a platform vendor underprice best-of-breed SIEM on data economics.
- **Participants.** Cisco (post-Splunk SIEM, XDR, Hypershield, AI Defense); the established best-of-breed SIEM cohort it is pressuring, including Microsoft Sentinel and the standalone SIEM positioning of CrowdStrike Falcon LogScale.
- **Conditional outcome.** *If Cisco's published earnings continue to report security revenue growth across the next two quarters, with Splunk-sourced platform attach as a named driver, we expect the data-OS framing to validate as a genuine telemetry-economics lever. If instead security revenue growth flattens, or Splunk recedes from the earnings narrative, the $28 billion bet reads as an expensive SIEM that has not yet rewritten the unit economics of the SOC.*
- **Evidence.** NetworkWorld, Cisco RSA Splunk integrations, 2026 (networkworld.com, accessed 2026-06-16); Cisco security revenue per fiscal Q4 reference figures (accessed 2026-06-16).

Play 3: The Agentic-SOC-Analyst Play

- **Observation.** The Tier-1 triage analyst is being targeted by autonomous AI agents across the field. Microsoft moved its Security Analyst Agent and Alert Triage Agent in Defender into preview at RSA 2026 in late March; email and collaboration alert triage is already generally available, and the agent is extending to identity and cloud alerts.[47] SentinelOne shipped Purple AI Auto-Investigations and reported roughly half of its $1,163 million ARR is now non-endpoint as of fiscal Q1 2027.[48] Dropzone AI, a venture-stage specialist, reports clearing roughly 90% of Tier-1 tickets with its AI SOC analyst, and is expanding from triage into threat hunting and intel with new agents launching in Q2 2026.[49]

- **Participants.** Microsoft (Security Copilot agents in Defender); SentinelOne (Purple AI Auto-Investigations); Dropzone AI (autonomous SOC analyst); cross-front overlap with the AI security thesis in Front 7.
- **Conditional outcome.** *If two or more of these vendors disclose that agentic triage is displacing measurable Tier-1 analyst workload at named enterprise accounts — on earnings calls or in named-outlet customer references — we expect "AI labor in the SOC" to move from product-page claim to a budgeted line item. If instead the agents stay framed as assistive copilots in vendor materials, with no customer-side workload-displacement reference, the play remains a productivity feature rather than a labor-model shift.*
- **Evidence.** Microsoft Tech Community, Security Copilot for SOC, 2026 (techcommunity.microsoft.com, accessed 2026-06-16); SentinelOne 10-Q, period ended 2026-04-30 (sec.gov, accessed 2026-06-16); Dropzone AI press release and SecurityWeek, $37M Series B, July 2025 (accessed 2026-06-16).

Play 4: The MDR-Boundary-Move Play

- **Observation.** Zscaler, an edge-security vendor, acquired the managed detection and response provider Red Canary for roughly $651.4 million, completed on August 1, 2025.[50] The move pulls a pure-play SSE vendor across the boundary into detection and response, the core territory of this front. Zscaler's own scale gives it room to do so: Q3 FY26 revenue near $850 million, up 25% year over year, with ARR around $3,525 million.[51]
- **Participants.** Zscaler (post-Red Canary MDR); the detection-and-response incumbents whose managed-service revenue it now contests, including CrowdStrike Falcon Complete and Microsoft's managed Defender services; cross-front overlap with the edge analysis in Front 6.
- **Conditional outcome.** *If Zscaler's earnings calls over the next two quarters cite Red Canary MDR as a named attach or cross-sell driver against its SSE base, we expect edge vendors crossing into detection and response to become a recurring acquisition pattern rather than a one-off. If instead Red Canary stays a quiet line item with no cross-sell narrative, the deal reads as a capability tuck-in, not a boundary move.*
- **Evidence.** Zscaler 10-Q, period ended 2026-04-30 (sec.gov, accessed 2026-06-16); Red Canary acquisition completed 2025-08-01 (Zscaler press release, accessed 2026-06-16).

5.5 War Chests & Casualties

The capital picture for this front splits cleanly into two groups: public incumbents financing consolidation off their own balance sheets, and privately held specialists whose last fundraises range from very recent to several years old. The snapshot below mixes both. For deeper venture-landscape analysis across all fronts, see the Phase 3 convergence chapter.

Vendor	Most Recent Round	Valuation (if public)	Strategic Investor	Distress Signal
Palo Alto Networks (NASDAQ: PANW)	Public; deployed ~$25B (CyberArk, closed 2026-02-11) + ~$3.35B (Chronosphere, closed Jan 2026)[52]	Public market cap	Public-market funded	(empty — no public distress event)
CrowdStrike (NASDAQ: CRWD)	Public; ~$4.5B cash and equivalents, FY26 Q1; ongoing tuck-in M&A[53]	Public market cap	Public-market funded	(empty — no public distress event)
SentinelOne (NYSE: S)	Public; ~$1,163M ARR (+23% YoY), fiscal Q1 2027; acquired Prompt Security + Observo[54]	Public market cap	Public-market funded	(empty — no public distress event)
Cisco (NASDAQ: CSCO)	Public; ~$28B Splunk integration deepening; security revenue ~$1.95B/quarter[55]	Public market cap	Public-market funded	(empty — no public distress event)
Vectra AI (private)	~$425M raised across ~15 rounds; acquired Netography (terms undisclosed)[56]	~$1.2B (private, last reported)	Venture-backed unicorn	(empty — no public distress event)
Dropzone AI (private)	$37M Series B, July 2025 (Theory Ventures; Madrona, Decibel, PSL, IQT)[57]	Not disclosed	Theory Ventures (lead); IQT	(empty — no public distress event)
Hunters (private)	$68M Series C, January 2022; ~$118M total raised. No newer round on public record[58]	Not disclosed	Venture-backed	(empty — no public distress event)

The dynamic is asymmetric. The public players are spending balance-sheet cash to buy adjacencies into the SOC platform: Palo Alto bought identity and observability, Cisco bought the data layer, and CrowdStrike and SentinelOne are funding tuck-ins from cash and growing ARR. The privately held specialists divide by capital recency. Dropzone AI raised fresh capital in mid-2025 and is expanding scope on the strength of it. Vectra AI sits on a unicorn valuation and used it to acquire Netography. Hunters, by contrast, last raised publicly in January 2022, and no newer round appears on the public record, so any read of its position should rest on its standalone SIEM-replacement traction rather than on implied capital. None of the seven carries a citable public distress event in this snapshot. Cybereason's reported 2023–2024 down-round narrative is the nearest distress candidate in this segment, but it is not a top-eight contender here and is left out of this table rather than labeled without a same-paragraph dated source.[59]

5.6 Winning & Losing

The SOC platform war is the most contested ground in the entire report, and it is contested on two axes at once. The first axis is the endpoint battlefield proper: who owns the agent on the box, the detections it fires, and the analyst workflow that triages them. The second axis is the SIEM battlefield above it: who owns the data lake, the correlation engine, and the economics of ingesting everything an enterprise generates. For a decade these were separate fights with separate winners. In 2026 they are collapsing into one, and the vendors who win the collapse are the ones who can credibly tell a buyer "one platform, one console, one bill" without that promise falling apart under the weight of telemetry costs.

Three patterns explain who is advancing and who is dug in. The first is a clean segmentation line opening up between an AI-native challenger and the scaled incumbent. The second is the platform pressure a bundled-by-default SOC plane exerts on every standalone vendor below it. The third is the absorption test that will decide whether platform consolidation can actually replace best-of-breed SIEM, or whether telemetry economics quietly defeat the consolidation pitch. Each is a falsifiable thesis, not a forecast — I have named the public signal that would confirm or refute it by the next refresh.

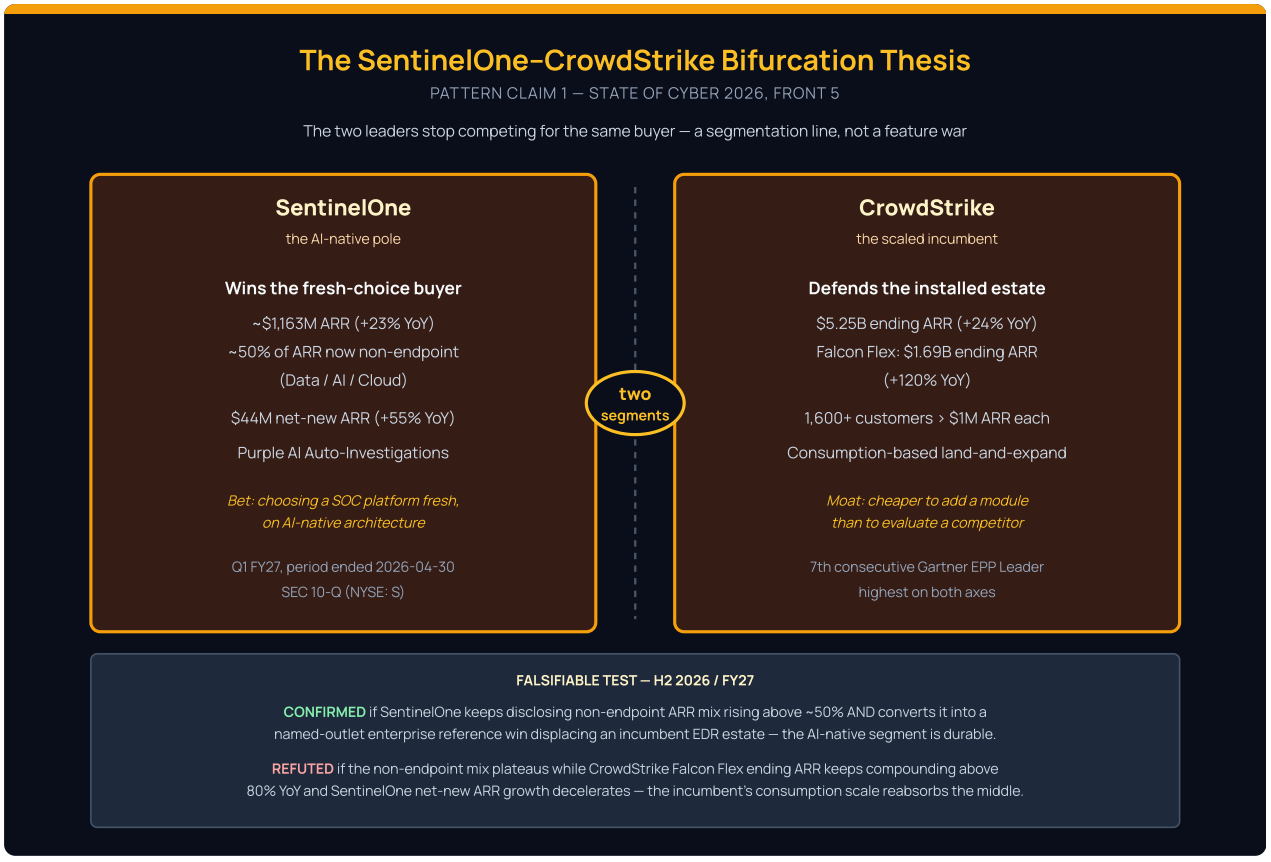
Pattern Claim 1 — The SentinelOne–CrowdStrike Bifurcation Thesis

Observation. - SentinelOne reported Q1 FY27 (period ended 2026-04-30) ARR of $1,163M, up 23% year-over-year, and disclosed that roughly 50% of total company ARR now comes from non-endpoint solutions — Data, AI, and Cloud — a milestone the company framed as its emerging solutions reaching half of total ARR [60]. - In the same period it launched Purple AI Auto-Investigations, positioning autonomous triage as a headline capability [60]. - CrowdStrike, over the same window, crossed $5.25B ending ARR at 24% year-over-year growth, with its Falcon Flex consumption model reaching $1.69B in ending ARR (up over 120% year-over-year) across more than 1,600 customers averaging over $1M in ARR each [61]. - Both vendors are named Leaders in the 2026 Gartner Magic Quadrant for Endpoint Protection Platforms — CrowdStrike for the seventh consecutive year and positioned highest in both axes, SentinelOne for the sixth [62].

My read. - I read this as the two vendors no longer competing for the same buyer with the same pitch. - CrowdStrike is selling scale and consolidation-by-consumption: Falcon Flex is a land-and-expand instrument that lets a large enterprise pre-commit a budget and draw down modules. - The 120%+ Flex growth tells me the incumbent's moat is increasingly commercial — the buyer who has standardized on Falcon finds it cheaper to add a module than to evaluate a competitor. - SentinelOne's 50%-non-endpoint mix is a different bet: it is trying to win the buyer who is choosing a SOC platform fresh, on AI-native architecture and data/cloud breadth, rather than the buyer defending an installed Falcon estate. - These are becoming two distinct buyer segments, and the AI-native-versus-incumbent framing is starting to function as a clean segmentation line rather than a feature war.

Conditional prediction. - The bifurcation is real and durable if SentinelOne's H2 2026 and FY27 earnings continue to disclose a rising non-endpoint ARR mix (above the ~50% Q1 mark) AND it converts that into named-outlet enterprise reference wins displacing an incumbent EDR estate. That would show the AI-native segment is large enough to sustain a public pure-play. - If instead the non-endpoint mix plateaus, and CrowdStrike's Falcon Flex ending ARR keeps compounding above 80% year-over-year while SentinelOne's net-new ARR growth decelerates, then the "bifurcation" is a transitional artifact, and the incumbent's consumption-model scale reabsorbs the contested middle.

Sources. [60] [61] [62]


The SentinelOne–CrowdStrike Bifurcation Thesis
PATTERN CLAIM 1 — STATE OF CYBER 2026, FRONT 5
The two leaders stop competing for the same buyer — a segmentation line, not a feature war
SentinelOne
the AI-native pole
Wins the fresh-choice buyer
~$1,163M ARR (+23% YoY)
~50% of ARR now non-endpoint
(Data / AI / Cloud)
$44M net-new ARR (+55% YoY)
Purple AI Auto-Investigations
Bet: choosing a SOC platform fresh, on AI-native architecture
Q1 FY27, period ended 2026-04-30
SEC 10-Q (NYSE: S)
two segments
CrowdStrike
the scaled incumbent
Defends the installed estate
$5.25B ending ARR (+24% YoY)
Falcon Flex: $1.69B ending ARR
(+120% YoY)
1,600+ customers > $1M ARR each
Consumption-based land-and-expand
Moat: cheaper to add a module than to evaluate a competitor
7th consecutive Gartner EPP Leader
highest on both axes
FALSIFIABLE TEST — H2 2026 / FY27
CONFIRMED if SentinelOne keeps disclosing non-endpoint ARR mix rising above ~50% AND converts it into a named-outlet enterprise reference win displacing an incumbent EDR estate — the AI-native segment is durable.
REFUTED if the non-endpoint mix plateaus while CrowdStrike Falcon Flex ending ARR keeps compounding above 80% YoY and SentinelOne net-new ARR growth decelerates — the incumbent's consumption scale reabsorbs the middle.

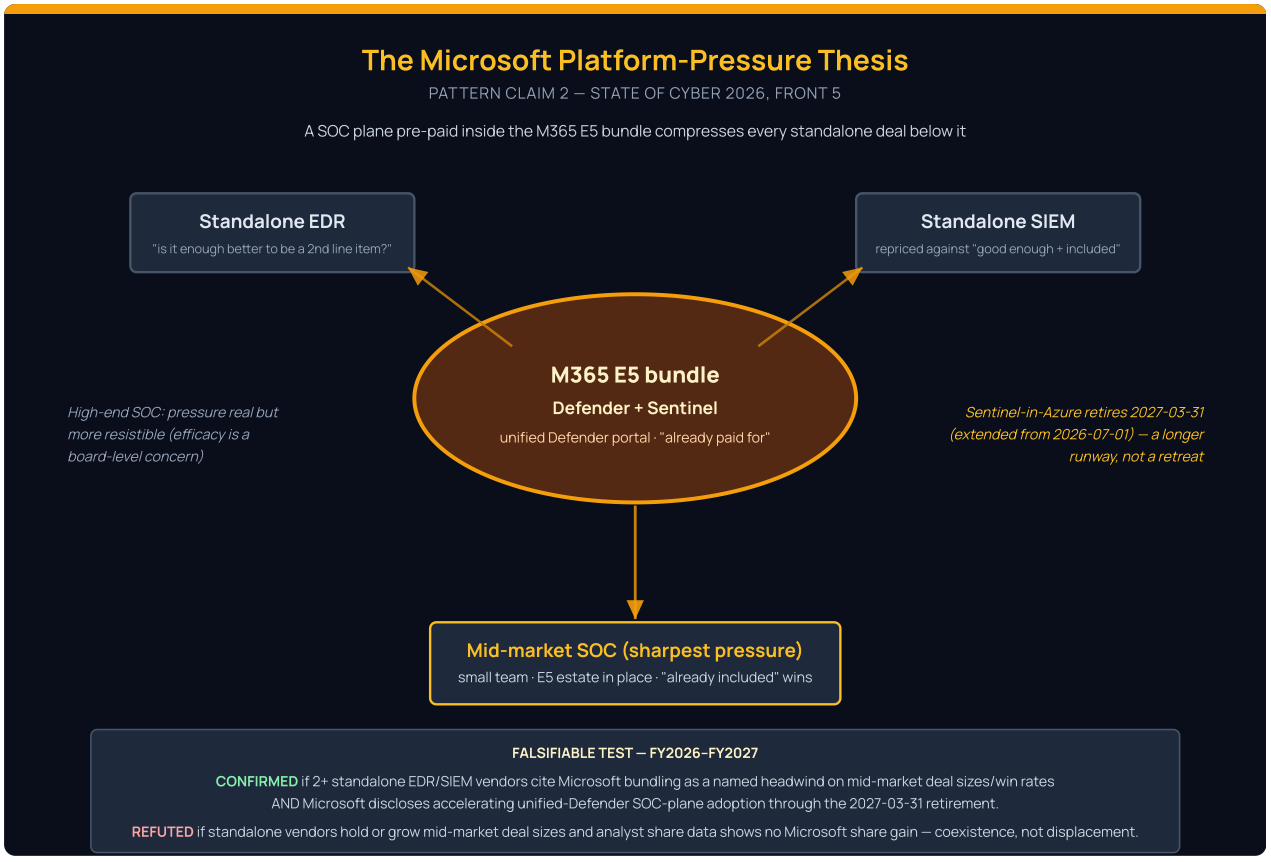
Pattern Claim 2 — The Microsoft Platform-Pressure Thesis

Observation. - In January 2026 Microsoft extended the retirement of the Microsoft Sentinel experience in the Azure portal from the original 2026-07-01 date to 2027-03-31, after which all SIEM and SOAR capabilities will operate exclusively inside the Microsoft Defender portal [63]. - Microsoft describes the unified Defender portal as the foundation for a single SOC operating model built on a two-tier data architecture, graph-based investigation, and AI agents. - New Sentinel instances created after August 2025 already default to the Defender portal [63]. - This consolidation rides on the M365 E5 commercial bundle, where Defender and Sentinel reach the buyer as part of a license the enterprise has frequently already purchased for productivity and identity reasons.

My read. - I read the deadline extension not as a retreat but as the opposite — Microsoft is in no hurry because the bundle does the selling. - When a SOC plane arrives effectively pre-paid inside an E5 agreement, the competitive question for a standalone EDR or SIEM vendor stops being "is your product better" and becomes "is your product enough better to justify a second line item the buyer could fold into a license they already hold." - My view is that this pressure is sharpest at the mid-market, where security teams are smaller, the E5 estate is already in place, and the marginal appeal of "good enough and already included" is highest. - At the high end, where SOC teams are large and best-of-breed detection efficacy is a board-level concern, the bundle pressure is real but more resistible. - The extended runway to 2027-03-31 simply gives Microsoft a longer window to convert E5 holders to the single Defender plane before standalone vendors can reprice against it.

Conditional prediction. - The thesis is confirmed if two conditions hold together: two or more standalone EDR/SIEM vendors cite Microsoft bundling as a named headwind in their FY2026–FY2027 earnings commentary on deal sizes or mid-market win rates, AND Microsoft discloses accelerating adoption of the unified Defender SOC plane through the 2027-03-31 retirement. In that case the standalone mid-market deal economics compress. - If instead standalone vendors hold or grow mid-market deal sizes through the retirement window, and analyst share data shows no Microsoft share gain at the standalone vendors' expense, the bundle is a coexistence story, not a displacement one, and the pressure thesis is overstated.

Sources. [63] [64]


The Microsoft Platform-Pressure Thesis
PATTERN CLAIM 2 — STATE OF CYBER 2026, FRONT 5
A SOC plane pre-paid inside the M365 E5 bundle compresses every standalone deal below it
Standalone EDR
"is it enough better to be a 2nd line item?"
Standalone SIEM
repriced against "good enough + included"
M365 E5 bundle
Defender + Sentinel
unified Defender portal · "already paid for"
High-end SOC: pressure real but more resistible (efficacy is a board-level concern)
Sentinel-in-Azure retires 2027-03-31 (extended from 2026-07-01) — a longer runway, not a retreat
Mid-market SOC (sharpest pressure)
small team · E5 estate in place · "already included" wins
FALSIFIABLE TEST — FY2026–FY2027
CONFIRMED if 2+ standalone EDR/SIEM vendors cite Microsoft bundling as a named headwind on mid-market deal sizes/win rates AND Microsoft discloses accelerating unified-Defender SOC-plane adoption through the 2027-03-31 retirement.
REFUTED if standalone vendors hold or grow mid-market deal sizes and analyst share data shows no Microsoft share gain — coexistence, not displacement.

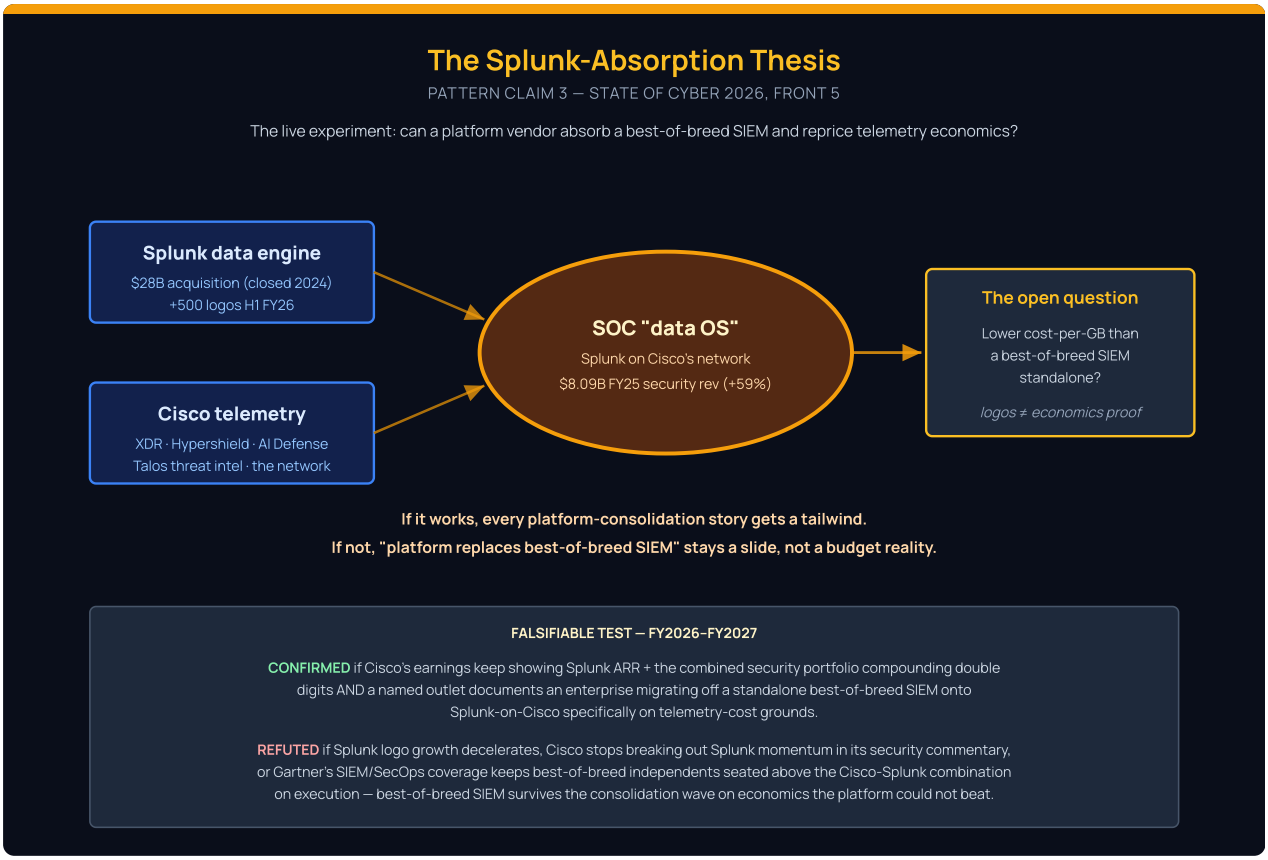
Pattern Claim 3 — The Splunk-Absorption Thesis

Observation. - Cisco's $28B acquisition of Splunk closed in 2024, and through FY2026 Cisco has been integrating Splunk's SIEM, SOAR, and observability layer with its own network telemetry [65]. - Cisco reported that Splunk added 500 new logos in H1 FY26 and was on pace for 1,000 by year-end, with ARR and product RPO both growing double digits, while the combined Cisco-Splunk security portfolio added 750 new customers in a single quarter across Secure Access, XDR, Hypershield, and AI Defense [66]. - Cisco's security business reached $8.09B in fiscal 2025 revenue, up 59% from the prior year, and roughly 19.5% of total revenue, with Q3 FY26 (period ended 2026-04-25) total revenue of $15.8B [65] [66]. - That 59% jump largely reflects Splunk's first full fiscal year folded into the security segment, and is therefore substantially inorganic.

My read. - I read the Cisco-Splunk integration as the single most important live experiment in the SIEM market. - It tests the proposition the entire consolidation pitch rests on: that a platform vendor can absorb a best-of-breed SIEM and reprice telemetry economics in the buyer's favor by pairing data ingestion with the network it already owns. - My view is that the logo growth is real but not yet the proof point — adding 500 new Splunk logos shows Cisco can sell Splunk, not that Cisco has solved the cost-of-ingestion problem that makes standalone SIEM painful. - The thesis is decided not by how many logos the combined entity wins, but by whether Cisco can credibly tell a buyer that running Splunk on Cisco telemetry costs materially less per gigabyte than running a best-of-breed SIEM standalone. - If it can, every other platform consolidation story in this front gets a tailwind. If it cannot, "platform replaces best-of-breed SIEM" stays a slide, not a budget reality.

Conditional prediction. - The absorption is working if two things hold: Cisco's FY2026–FY2027 earnings disclosures continue to show Splunk ARR and the combined security portfolio compounding double digits, AND a named outlet documents an enterprise migrating off a standalone best-of-breed SIEM onto Splunk-on-Cisco specifically on telemetry-cost grounds. In that case platform consolidation has a credible answer to the ingestion-economics objection. - If instead Splunk logo growth decelerates, Cisco stops breaking out Splunk momentum in its security commentary, or Gartner's SIEM/SecOps coverage continues to seat best-of-breed independents above the Cisco-Splunk combination on execution, the absorption has stalled, and best-of-breed SIEM survives the consolidation wave on economics the platform could not beat.

Sources. [65] [66]



Winners

CrowdStrike is winning the commercial dimension of this war. Crossing $5.25B ending ARR at 24% growth with Falcon Flex ending ARR up over 120% year-over-year is, in my read, the clearest evidence in the front that a consumption-based consolidation model can lock in an installed base while still expanding it [61]. The seventh consecutive Gartner EPP Leader placement — positioned highest on both Ability to Execute and Completeness of Vision — confirms the analyst community sees no erosion of the core franchise even as the company pushes into AI detection-and-response and the agentic interaction layer [62] [67]. My opinion: CrowdStrike's moat in 2026 is as much commercial architecture (Flex) as it is detection efficacy.

SentinelOne is winning the repositioning it set out to win. Reaching ~50% non-endpoint ARR while sustaining 23% ARR growth and posting a company-record $44M in net-new ARR (up 55% year-over-year) is, in my view, the strongest available public evidence that the AI-native platform narrative is converting to revenue rather than just messaging [60]. It is not winning at CrowdStrike's scale, but it is winning the argument that a public pure-play can credibly anchor the AI-native segment.

Microsoft is winning by default-distribution. I read the deliberate, unhurried extension of the Defender-portal consolidation to 2027-03-31 as the move of a vendor that does not need to rush because the E5 bundle keeps compounding its reach into the SOC regardless of release cadence [63]. The seventh consecutive EPP Leader placement removes the "good enough but not a Leader" objection that once let standalone vendors hold the line [62].

Losers / Casualties

Cybereason is the front's clearest casualty. Its valuation collapsed roughly 90% from $3.3B in July 2021 to about $300M by April 2023, it ran a third round of layoffs in March 2024 that included the exit of its product and R&D head, and it saw a CEO transition in 2025 [68]. Its proposed merger with MDR provider Trustwave, announced November 2024, was subsequently terminated [68]. Each of those is a dated public event; together they describe a vendor that has lost the scale race in the EDR tier and has not found a consolidation lifeline.

The SIEM-tier consolidation has produced one large defensive combination rather than a clear casualty: the **Exabeam–LogRhythm** merger completed July 17, 2024, and was accompanied by layoffs of 80 workers in Broomfield as the merged entity rationalized two overlapping SIEM portfolios [69]. I would not label the merged Exabeam a casualty — it is a consolidation play with a credible pure-play SecOps pitch — but the layoffs are the dated evidence that the standalone-SIEM middle is under genuine pressure, consistent with the Microsoft platform-pressure and Splunk-absorption theses above.

Watch

Hunters is the watch signal I would track most closely on funding cadence. Its most recent verifiable round remains the $68M Series C from January 2022 (~$118M total raised); no newer raise has surfaced [70]. For a SIEM-replacement SOC platform competing against Cisco-Splunk, Microsoft, and CrowdStrike's LogScale, a four-year gap since the last public round is a signal worth watching. It is not a distress label, but a cadence that would warrant reassessment at the next refresh if it extends through 2026 without a new round or a strategic outcome.

Dropzone AI is the agentic-SOC wildcard scaling into the thesis. Its $37M Series B (July 2025, Theory Ventures) funds an expansion from triage-only into full-spectrum detection with AI Threat Hunter and AI Threat Intel Analyst agents launching in Q2 2026 [71]. Whether the autonomous-SOC-analyst category becomes a feature absorbed by the platforms or a standalone wedge is the open question; Dropzone's capability expansion is the public signal to watch.

Vectra AI is worth watching post-Netography. Its acquisition of Netography (terms undisclosed) nudges it from AI-driven NDR toward converged cloud network observability, and it was named a Leader in the 2026 Gartner Magic Quadrant for NDR for the second consecutive year [72]. The watch question is whether behavior-first NDR remains a distinct analytical contender or gets pulled into the converging XDR/SOC-platform gravity well the three Pattern Claims describe.

5.7 The Campaign Ahead

The SOC platform war will be decided in public over the next several quarters, and the signals that decide it are observable without privileged access. These are the five I would put on the H2 2026 watchlist, each with a falsifiable threshold and a primary source class anyone can monitor.

1. **The non-endpoint ARR mix at the AI-native pure-play.** Signal: SentinelOne's quarterly earnings disclosures of non-endpoint (Data/AI/Cloud) ARR as a share of total ARR. Threshold: if the non-endpoint share rises above the ~50% Q1 FY27 mark across two consecutive quarters, the AI-native segment is structurally expanding; if it plateaus or reverses, the bifurcation thesis weakens. Primary source: SentinelOne (NYSE: S) earnings transcripts and 10-Q filings [73].
2. **The Microsoft Defender single-SOC-plane unification at the retirement date.** Signal: Microsoft's disclosures on unified Defender-portal SOC adoption as the 2027-03-31 Sentinel-in-Azure retirement approaches, plus any standalone-vendor earnings commentary naming Microsoft bundling as a deal-size headwind. Threshold: if two or more standalone EDR/SIEM vendors cite Microsoft bundle pressure on mid-market deal economics in earnings commentary, the platform-pressure thesis is confirmed. Primary source: Microsoft Security blog/Tech Community posts and standalone-vendor earnings transcripts [74].
3. **Cisco-Splunk telemetry-economics repricing.** Signal: Cisco's security-segment and Splunk-momentum disclosures in FY2026–FY2027 earnings, plus any named-outlet report of an enterprise migrating off standalone best-of-breed SIEM onto Splunk-on-Cisco on cost-of-ingestion grounds. Threshold: a documented best-of-breed-SIEM-to-Splunk-on-Cisco migration cited specifically on telemetry economics confirms the absorption thesis; continued logo growth without an economics proof point does not. Primary source: Cisco (NASDAQ: CSCO) earnings transcripts and named-outlet enterprise coverage [75].
4. **The agentic-SOC GA milestone.** Signal: general-availability launches of autonomous-SOC-analyst capabilities across the front — Dropzone's AI Threat Hunter and AI Threat Intel Analyst agents (slated Q2 2026), CrowdStrike's agentic interaction-layer protection, SentinelOne's Purple AI Auto-Investigations, and Microsoft's Defender AI agents. Threshold: if three or more contenders ship GA agentic-SOC capabilities as a headline product-page hero by year-end, autonomous triage has crossed from differentiator to table stakes. Primary source: vendor product-page hero snapshots and funding/launch announcements [76].
5. **CrowdStrike's Falcon Flex consumption trajectory.** Signal: CrowdStrike's quarterly disclosure of Falcon Flex ending ARR and account count. Threshold: if Flex ending ARR growth stays above 80% year-over-year through FY2027, the consumption-based bundling moat is widening and the contested middle reabsorbs toward the incumbent; if Flex growth decelerates sharply, the AI-native challenger has more room than the bifurcation's incumbent branch assumes. Primary source: CrowdStrike (NASDAQ: CRWD) earnings transcripts and 8-K exhibits [77].

References & Footnotes

1. EDR definition and device-level behavioral detection scope. Mordor Intelligence, "Endpoint Detection and Response (EDR) Market," accessed 2026-06-16. https://www.mordorintelligence.com/industry-reports/endpoint-detection-and-response-market ↩

2. XDR cross-domain correlation definition. Fortune Business Insights, “Extended Detection and Response Market,” accessed 2026-06-16. https://www.fortunebusinessinsights.com/extended-detection-and-response-market-105900 ↩

3. SIEM definition (log ingestion, correlation analytics, retention). Splunk, “SIEM: Security Information & Event Management Explained,” accessed 2026-06-16. https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html ↩

4. Unification of EDR/XDR/SIEM into a single next-generation SOC plane, including the data lake sitting beneath XDR rather than retiring the SIEM tier. Microsoft, “Microsoft Sentinel — AI-Ready Platform,” accessed 2026-06-16. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel/ ↩↩

5. Shared-substrate framing (SOC platforms consume IRM/DLP/DSPM/SSE/Identity signals and own the unified case timeline; per-front platforms own depth in their own primitive). State of Cyber Security Markets 2026, taxonomy §2.4. ↩

6. Telemetry volume as a cost driver rather than a value driver, motivating the SIEM repricing tension. Marketsandmarkets, “Security Information and Event Management Market Report 2026-2031,” accessed 2026-06-16. https://www.marketsandmarkets.com/Market-Reports/security-information-event-management-market-183343191.html ↩

7. Correlation, detection-engineering, and AI-investigation layers riding atop the SIEM are where product value and lock-in live. SentinelOne, “Purple AI | AI Security Analyst for Autonomous SecOps,” accessed 2026-06-16. https://www.sentinelone.com/platform/purple/ ↩

8. EDR market at ~USD 6.33B (2026), projected ~USD 18.68B by 2031 at ~24.15% CAGR; broader Endpoint Protection Platform framing ~USD 7.23B (2026); U.S. federal civilian agency EDR deployment mandates extending into cloud and identity coverage. Mordor Intelligence, “Endpoint Detection and Response (EDR) Market,” accessed 2026-06-16, https://www.mordorintelligence.com/industry-reports/endpoint-detection-and-response-market ; Fortune Business Insights, “Endpoint Detection and Response Market,” accessed 2026-06-16, https://www.fortunebusinessinsights.com/endpoint-detection-and-response-market-107235 ↩↩

9. SIEM market at USD 8.39B (2026) → USD 13.67B by 2031 at ~10.3% CAGR (Marketsandmarkets); USD 12.06B (2026) (Mordor Intelligence). Marketsandmarkets, accessed 2026-06-16, https://www.marketsandmarkets.com/Market-Reports/security-information-event-management-market-183343191.html ; Mordor Intelligence, “Security Information and Event Management Market,” accessed 2026-06-16, https://www.mordorintelligence.com/industry-reports/global-security-information-and-event-management ↩

10. XDR market estimates for 2026 range from ~USD 1.99B–2.56B (conservative) to high-single-digit billions (aggressive), all at >20% CAGR. Straits Research, “Extended Detection and Response Market,” accessed 2026-06-16, https://straitsresearch.com/report/extended-detection-and-response-market ; Fortune Business Insights, “Extended Detection and Response Market,” accessed 2026-06-16, https://www.fortunebusinessinsights.com/extended-detection-and-response-market-105900 ↩

11. Platform consolidation as the dominant procurement shift; unified analyst workflow as the buyer-side rationale. MarketsandMarkets Blog, “Extended Detection and Response Market — Driving Factors,” accessed 2026-06-16. https://web.archive.org/web/2*/https://www.marketsandmarketsblog.com/extended-detection-and-response-market-driving-factors-industry-growth-key-vendors-and-forecasts-to-2030.html ↩

12. Growth of managed/co-managed SOC operations (SOC-as-a-service, MDR) driven by analyst-talent shortage. The Business Research Company, “SOC as a Service Global Market Report,” accessed 2026-06-16. https://www.thebusinessresearchcompany.com/report/soc-as-a-service-global-market-report ↩

13. SentinelOne Purple AI attached to over 50% of all licenses sold in Q4 FY26; general availability of one-click agentic Auto-Investigation with analyst-in-the-loop governance, announced at RSAC 2026. SentinelOne, “SentinelOne Unveils New AI Security Offerings to Give Defenders a Decisive Advantage,” 2026-03-23, accessed

2026-06-16. https://www.sentinelone.com/press/sentinelone-unveils-new-ai-security-offerings-to-give-defenders-a-decisive-advantage/ ↩

14. Dropzone AI autonomous SOC-analyst positioning, ~100+ customers, expansion from triage to threat hunting/intel in Q2 2026. SecurityWeek, "Dropzone AI Raises $37 Million for Autonomous SOC Analyst," accessed 2026-06-16. https://www.securityweek.com/dropzone-ai-raises-37-million-for-autonomous-soc-analyst/ ↩

15. Microsoft Sentinel data lake with generally available lake-only ingestion for Defender advanced-hunting tables; Defender portal positioned as single SOC plane with embedded Security Copilot agents. Microsoft Community Hub, "What's new in Microsoft Sentinel: February 2026," accessed 2026-06-16. https://techcommunity.microsoft.com/blog/microsoftsentinelblog/what%E2%80%99s-new-in-microsoft-sentinel-february-2026/4494218 ↩

16. Telemetry-cost pressure repricing the SIEM; Cisco's Splunk-as-data-platform integration as the largest decoupling bet. Network World, "At RSA, Cisco unveils Splunk integrations, Hypershield upgrades," accessed 2026-06-16. https://www.networkworld.com/article/2098349/at-rsa-cisco-unveils-splunk-integrations-hypershield-upgrades.html ↩

17. Microsoft extended the retirement of the Sentinel experience in Azure (transition to the Defender portal) to 2027-03-31, from a prior 2026-07-01 date. Microsoft Community Hub, "Update: New timeline for transitioning Sentinel experience to Defender portal," accessed 2026-06-16. https://techcommunity.microsoft.com/blog/microsoftsentinelblog/update-new-timeline-for-transitioning-sentinel-experience-to-defender-portal/4490464 ↩

18. SEC Form 8-K Item 1.05 requires disclosure of a material cybersecurity incident within four business days of the materiality determination (not discovery). SEC, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" small-business compliance guide, accessed 2026-06-16. https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure ↩

19. CrowdStrike Falcon platform page, hero messaging "The Agentic Security Platform. Unified and built to secure the AI revolution." https://www.crowdstrike.com/en-us/platform/ (accessed 2026-06-16). ↩

20. CrowdStrike Falcon platform page, core value proposition: "The AI era is transforming cybersecurity across three critical fronts — and the CrowdStrike Falcon Platform secures them all." https://www.crowdstrike.com/en-us/platform/ (accessed 2026-06-16). ↩

21. CrowdStrike Holdings, Form 10-Q for the period ended 2026-04-30 (fiscal Q1 2026): cash and equivalents ~$4.5B; ongoing business acquisitions reflect tuck-in M&A; George Kurtz President/CEO/Director. https://www.sec.gov/Archives/edgar/data/0001535527/000153552726000025/crwd-20260430.htm (accessed 2026-06-16). ↩

22. Microsoft Defender business page, hero pillar: "Prevent and disrupt threats with AI-powered, coordinated defense." https://www.microsoft.com/en-us/security/business/microsoft-defender (accessed 2026-06-16). ↩

23. Microsoft Sentinel page, pillar: "Power your agentic defense with unified data and context." https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel (accessed 2026-06-16). ↩

24. Microsoft Sentinel page, product descriptor "cloud-native SIEM that unifies AI, SOAR, UEBA, and TI"; unified data lake and intelligent reasoning tools; Security Copilot agents. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel (accessed 2026-06-16). ↩

25. Microsoft, "Update: New timeline for transitioning the Sentinel experience to the Defender portal" — retirement of the legacy Sentinel-in-Azure experience extended to 2027-03-31 (from the earlier 2026-07-01 target). https://techcommunity.microsoft.com/blog/microsoftsentinelblog/update-new-timeline-for-transitioning-sentinel-experience-to-defender-portal/4490464 (accessed 2026-06-16). ↩

26. SentinelOne homepage, hero “Built to Secure. Engineered for Advantage.” and pillar “AI-native security powered by Autonomous Security Intelligence. See further. Stop faster. Gain the edge.” https://www.sentinelone.com/ (accessed 2026-06-16). ↩↩

27. SentinelOne, Form 10-Q for the period ended 2026-04-30 (fiscal Q1 2027): ARR ~$1,163M (+23% YoY), revenue ~$277M; ~50% of ARR from non-endpoint (Data/AI/Cloud) products. https://www.sec.gov/Archives/edgar/data/0001583708/000158370826000041/s-20260430.htm (accessed 2026-06-16). ↩

28. SentinelOne acquisitions of Prompt Security (closed 2025-09-05) and Observo (closed 2025-09-22), AI-pipeline/AI-security tuck-ins; Purple AI Auto-Investigations. https://www.calcalistech.com/ctechnews/article/syo5r20kgl (accessed 2026-06-16). ↩

29. Palo Alto Networks Cortex XSIAM page, hero “Unlock true AI-driven security operations” and tagline “Unparalleled data. Unbeatable AI. The most advanced SOC platform.” https://www.paloaltonetworks.com/cortex/cortex-xsiam (accessed 2026-06-16). ↩

30. Palo Alto Networks Cortex XSIAM page, future-state framing “Unleash machine speed and precision with the autonomous SOC built to stop tomorrow’s threats.” https://www.paloaltonetworks.com/cortex/cortex-xsiam (accessed 2026-06-16). ↩

31. Palo Alto Networks completed its CyberArk acquisition (~$25B, identity security) on 2026-02-11 and its Chronosphere acquisition (~$3.35B, cloud-native observability) in January 2026; Cortex AgentiX integrated with Chronosphere for agentic find-and-fix. https://www.paloaltonetworks.com/company/press/2026/palo-alto-networks-completes-chronosphere-acquisition–unifying-observability-and-security-for-the-ai-era ; https://www.verdict.co.uk/palo-alto-networks-cyberark-deal/ (accessed 2026-06-16). ↩

32. Splunk Enterprise Security page (Splunk is a Cisco company), hero “Tired of disconnected tools? Meet the new standard for threat detection, investigation, and response (TDIR).” https://www.splunk.com/en_us/products/enterprise-security.html (accessed 2026-06-16). ↩

33. Cisco completed its acquisition of Splunk (~$28B) in 2024, reshaping the SIEM landscape. https://www.networkworld.com/article/2098349/at-rsa-cisco-unveils-splunk-integrations-hypershield-upgrades.html (accessed 2026-06-16). ↩

34. Splunk Enterprise Security page, pillar “Enterprise Security (ES) is a unified TDIR platform — seamlessly integrated with agentic AI, SOAR, UEBA, and SIEM”; Cisco wraps Splunk with Cisco XDR, Hypershield, and AI Defense. https://www.splunk.com/en_us/products/enterprise-security.html (accessed 2026-06-16). ↩

35. Cisco security revenue ~$1.95B/quarter (+9% YoY, FY25 Q4 reference); newer security products (Secure Access, XDR, Hypershield, AI Defense) ~5,000 cumulative customers. https://www.networkworld.com/article/2098349/at-rsa-cisco-unveils-splunk-integrations-hypershield-upgrades.html (accessed 2026-06-16). ↩

36. Vectra AI homepage, taglines “AI-native, not AI nonsense” and “We protect modern networks from modern attacks. Vectra AI sees attackers’ every move, connecting the dots across network, identity, and cloud.” https://www.vectra.ai/ (accessed 2026-06-16). ↩↩

37. Vectra AI named a Leader in the 2026 Gartner Magic Quadrant for NDR (second consecutive year); acquired Netography (cloud-native network observability, terms undisclosed); private unicorn ~$1.2B valuation, ~$425M raised. https://securitybuzz.com/industry-news/vectra-ais-netography-acquisition-marks-a-new-era-for-ai-driven-network-defense/ ; https://www.vectra.ai/about/news (accessed 2026-06-16). ↩

38. Hunters homepage, hero “AI-Driven Next-Gen SIEM” with “Automated detection, investigation & response for small SecOps teams” and “A SIEM that works for you, not the other way around.” https://www.hunters.security/ (accessed 2026-06-16). ↩↩

39. Hunters most recent verifiable funding round: $68M Series C (January 2022; ~$118M total raised). No newer round surfaced in bounded scan. https://www.hunters.security/newsroom/hunters-secures-68-million-in-series-c-funding-to-become-a-leading-security-operations-platform-1 ; https://www.crunchbase.com/organization/hunters-ai (accessed 2026-06-16). ↩

40. Dropzone AI homepage, hero "Reinforce your SOC with AI Analysts" and "Hunt, investigate, and respond at machine scale"; "Dropzone's Agentic SOC continuously adapts your detection and response"; "The AI SOC analyst replicates the techniques of elite analysts to autonomously investigate and solve every alert." https://www.dropzone.ai/ (accessed 2026-06-16). ↩↩

41. Dropzone AI raised a $37M Series B (2025-07-17, led by Theory Ventures); 100+ customers; AI Threat Hunter + AI Threat Intel Analyst launching H1 2026. https://www.dropzone.ai/press-release/dropzone-ai-37m-series-b-funding-ai-soc-agents ; https://www.securityweek.com/dropzone-ai-raises-37-million-for-autonomous-soc-analyst/ (accessed 2026-06-16). ↩

42. Palo Alto Networks, "Palo Alto Networks Completes Chronosphere Acquisition — Unifying Observability and Security for the AI Era," 2026, https://www.paloaltonetworks.com/company/press/2026/palo-alto-networks-completes-chronosphere-acquisition–unifying-observability-and-security-for-the-ai-era (accessed 2026-06-16); Verdict, "Palo Alto Networks–CyberArk deal," 2026, https://www.verdict.co.uk/palo-alto-networks-cyberark-deal/ (accessed 2026-06-16). CyberArk close ~$25B (closed 2026-02-11); Chronosphere close ~$3.35B (closed January 2026). ↩

43. Palo Alto Networks, "Cortex AgentiX — Build, Deploy and Govern the Agentic Workforce of the Future," https://www.paloaltonetworks.com/cortex/agentix (accessed 2026-06-16). AgentiX integration with Chronosphere telemetry for agentic find-and-fix. ↩

44. Palo Alto Networks fiscal Q2 2026 earnings coverage, February 2026: XSIAM surpassed $500M ARR, 600+ customers, average ARR near $1M per customer, https://finance.yahoo.com/news/cortex-xsiam-become-palo-alto-142700968.html (accessed 2026-06-16). ↩

45. NetworkWorld, "At RSA, Cisco unveils Splunk integrations, Hypershield upgrades," 2026, https://www.networkworld.com/article/2098349/at-rsa-cisco-unveils-splunk-integrations-hypershield-upgrades.html (accessed 2026-06-16). Splunk acquired ~$28B, closed 2024; ThousandEyes, Hypershield, AppDynamics, AI Defense as first-class Splunk sources. ↩

46. Cisco security revenue ~$1.95B/quarter (+9% YoY, FY25 Q4 reference); newer security products ~5,000 cumulative customers, per NetworkWorld coverage, 2026, https://www.networkworld.com/article/2098349/at-rsa-cisco-unveils-splunk-integrations-hypershield-upgrades.html (accessed 2026-06-16). ↩

47. Microsoft Tech Community, "Security Copilot for SOC: bringing agentic AI to every defender," 2026, https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/security-copilot-for-soc-bringing-agentic-ai-to-every-defender/4470187 (accessed 2026-06-16); Microsoft Learn, "Security Alert Triage Agent in Microsoft Defender (Preview)," https://learn.microsoft.com/en-us/defender-xdr/security-alert-triage-agent (accessed 2026-06-16). Security Analyst Agent moved to preview at RSA 2026 (late March); email/collaboration alert triage generally available; extending to identity and cloud alerts. ↩

48. SentinelOne, Form 10-Q, period ended 2026-04-30, https://www.sec.gov/Archives/edgar/data/0001583708/000158370826000041/s-20260430.htm (accessed 2026-06-16). Fiscal Q1 2027 ARR ~$1,163M (+23% YoY); ~50% of ARR non-endpoint; Purple AI Auto-Investigations launched. ↩

49. Dropzone AI, "$37M Series B funding," 2025, https://www.dropzone.ai/press-release/dropzone-ai-37m-series-b-funding-ai-soc-agents (accessed 2026-06-16); SecurityWeek, "Dropzone AI Raises $37 Million for Autonomous SOC Analyst," 2025, https://www.securityweek.com/dropzone-ai-raises-37-million-for-autonomous-soc-analyst/ (accessed 2026-06-16). ~100+ customers; clears ~90% of Tier-1 tickets; AI Threat Hunter + AI Threat Intel Analyst launching Q2 2026. ↩

50. Zscaler, Form 10-Q, period ended 2026-04-30, https://www.sec.gov/Archives/edgar/data/0001713683/000171368326000096/zs-20260430.htm (accessed 2026-06-16). Red Canary (MDR) acquired ~$651.4M (10-Q purchase consideration), completed 2025-08-01. ↩

51. Zscaler Q3 FY26 (period ended 2026-04-30): revenue ~$850M (+25% YoY), ARR ~$3,525M, per Form 10-Q, https://www.sec.gov/Archives/edgar/data/0001713683/000171368326000096/zs-20260430.htm (accessed 2026-06-16). ↩

52. Palo Alto Networks (NASDAQ: PANW) deployed ~$25B for CyberArk (closed 2026-02-11) and ~$3.35B for Chronosphere (closed January 2026). Palo Alto Networks press release and Verdict, 2026, https://www.paloaltonetworks.com/company/press/2026/palo-alto-networks-completes-chronosphere-acquisition–unifying-observability-and-security-for-the-ai-era (accessed 2026-06-16). ↩

53. CrowdStrike (NASDAQ: CRWD), Form 10-Q, period ended 2026-04-30: cash and equivalents ~$4.5B; ~$382M business acquisitions (net of cash) reflecting ongoing tuck-in M&A, https://www.sec.gov/Archives/edgar/data/0001535527/000153552726000025/crwd-20260430.htm (accessed 2026-06-16). ↩

54. SentinelOne (NYSE: S), Form 10-Q, period ended 2026-04-30: ARR ~$1,163M (+23% YoY); acquired Prompt Security (~$133.6M, closed 2025-09-05) and Observo (~$130.2M, closed 2025-09-22), https://www.sec.gov/Archives/edgar/data/0001583708/000158370826000041/s-20260430.htm (accessed 2026-06-16). ↩

55. Cisco (NASDAQ: CSCO): Splunk (~$28B, closed 2024) integration deepening; security revenue ~$1.95B/quarter, per NetworkWorld, 2026, https://www.networkworld.com/article/2098349/at-rsa-cisco-unveils-splunk-integrations-hypershield-upgrades.html (accessed 2026-06-16). ↩

56. Vectra AI (private): ~$425M raised across ~15 rounds at a ~$1.2B valuation; acquired Netography (cloud network observability, terms undisclosed); named a Leader in the 2026 Gartner Magic Quadrant for NDR. SecurityBuzz, 2026, https://securitybuzz.com/industry-news/vectra-ais-netography-acquisition-marks-a-new-era-for-ai-driven-network-defense/ (accessed 2026-06-16); Vectra newsroom, https://www.vectra.ai/about/news (accessed 2026-06-16). ↩

57. Dropzone AI (private): $37M Series B, 2025-07-17, led by Theory Ventures (Madrona, Decibel, PSL, IQT participating). Dropzone AI press release, https://www.dropzone.ai/press-release/dropzone-ai-37m-series-b-funding-ai-soc-agents (accessed 2026-06-16). ↩

58. Hunters (private): $68M Series C, January 2022; ~$118M total raised. No newer round surfaced on the public record. Hunters newsroom, https://www.hunters.security/newsroom/hunters-secures-68-million-in-series-c-funding-to-become-a-leading-security-operations-platform-1 (accessed 2026-06-16); Crunchbase, https://www.crunchbase.com/organization/hunters-ai (accessed 2026-06-16). ↩

59. Cybereason (private) carried a reported down-round narrative in 2023–2024 per named-outlet coverage; it is not a top-eight contender in this front and is omitted from the War-Chest table rather than labeled a casualty without a current dated public event. Referenced as a documented omission in this front's vendor selection. ↩

60. SentinelOne Q1 FY27 results (period ended 2026-04-30): ARR $1,163M (+23% YoY), revenue $277M (+21%), ~50% of total ARR from non-endpoint (Data/AI/Cloud) solutions, record net-new ARR of $44M (+55% YoY), Purple AI Auto-Investigations launch. SentinelOne Form 8-K / Q1 FY27 earnings exhibit, accessed 2026-06-16. https://www.sec.gov/Archives/edgar/data/0001583708/000158370826000039/sentineloneq127exhibit991.htm ; Form 10-Q https://www.sec.gov/Archives/edgar/data/0001583708/000158370826000041/s-20260430.htm ↩↩↩↩

61. CrowdStrike FY2026 results: ending ARR $5.25B (+24% YoY); Falcon Flex ending ARR $1.69B (+120%+ YoY) across 1,600+ customers averaging $1M+ ARR; Falcon AI Detection and Response launched Q4 FY2026. CrowdStrike Form 8-K (FY2026 Q4), accessed 2026-06-16. https://www.sec.gov/Archives/edgar/data/0001535527/000153552726000007/crwd-20260303xex991.htm ↩↩↩

62. 2026 Gartner Magic Quadrant for Endpoint Protection Platforms named six Leaders, including CrowdStrike (7th consecutive year, positioned highest in both Ability to Execute and Completeness of Vision), SentinelOne (6th), Microsoft (7th), and Palo Alto Networks (4th). CrowdStrike blog, accessed 2026-06-16. https://www.crowdstrike.com/en-us/blog/crowdstrike-leader-in-2026-gartner-magic-quadrant-for-endpoint-protection/ ; MSSP Alert https://www.msspalert.com/feature/gartner-magic-quadrant-names-microsoft-sentinelone-among-epp-leaders ↩↩↩↩

63. Microsoft extended the Microsoft Sentinel Azure-portal retirement from 2026-07-01 to 2027-03-31 (announced January 2026); after that date all SIEM/SOAR capabilities operate exclusively in the Microsoft Defender portal, framed as a unified SOC plane with two-tier data architecture, graph-based investigation, and AI agents. New Sentinel instances post-August 2025 default to the Defender portal. Microsoft Tech Community, accessed 2026-06-16. https://techcommunity.microsoft.com/blog/microsoftsentinelblog/update-new-timeline-for-transitioning-sentinel-experience-to-defender-portal/4490464 ↩↩↩↩

64. Microsoft Security blog, "Migrate Sentinel to Defender — Why It Is a Security Architecture Decision, Not Just a Portal Change," accessed 2026-06-16. https://techcommunity.microsoft.com/blog/microsoft-security-blog/migrate-sentinel-to-defender—why-it-is-a-security-architecture-decision-not-ju/4513815 ↩

65. Cisco $28B Splunk acquisition (closed 2024) integrating Splunk SIEM/SOAR/observability with Cisco network telemetry; Cisco security revenue reached $8.09B in fiscal 2025 (+59% YoY, ~19.5% of total revenue); Q3 FY26 (period ended 2026-04-25) total revenue $15.8B. Cisco Form 8-K (Q3 FY2026 press release), accessed 2026-06-16. https://www.sec.gov/Archives/edgar/data/0000858877/000085887726000075/exhibit991pressrelease-q3f.htm ↩↩↩

66. Splunk added 500 new logos in H1 FY26 (on pace for 1,000 by year-end), ARR and product RPO growing double digits; combined Cisco-Splunk security portfolio added 750 new customers in a quarter across Secure Access, XDR, Hypershield, and AI Defense. Cybersecurity Dive, "Splunk accelerates Cisco's security business as core networking sales decline," accessed 2026-06-16. https://www.cybersecuritydive.com/news/splunk-growth-cisco-security/733196/ ↩↩↩

67. CrowdStrike launched Falcon AI Detection and Response in Q4 FY2026, positioning Falcon as the security layer for AI infrastructure across endpoints, cloud, identity, SaaS, browsers, and the agentic interaction layer. CrowdStrike Form 8-K (FY2026), accessed 2026-06-16. https://www.sec.gov/Archives/edgar/data/0001535527/000153552726000007/crwd-20260303xex991.htm ↩

68. Cybereason valuation fell ~90% from $3.3B (July 2021) to ~$300M (April 2023); third round of layoffs March 2024 affecting its product and R&D leadership; a CEO transition in 2025; proposed Trustwave merger (announced November 2024) terminated. BankInfoSecurity, "Cybereason CEO Eric Gan Out Following Scuffle With Investors," accessed 2026-06-16. https://www.bankinfosecurity.com/cybereason-ceo-eric-gan-out-following-scuffle-investors-a-27651 ↩↩

69. Exabeam and LogRhythm completed their merger 2024-07-17 (merged entity named Exabeam), accompanied by layoffs of 80 workers in Broomfield. BizWest, "Layoffs loom as LogRhythm, Exabeam complete merger," accessed 2026-06-16. https://bizwest.com/2024/07/17/layoffs-loom-as-logrhythm-exabeam-complete-merger/ ↩

70. Hunters' most recent verifiable round is its $68M Series C (January 2022; ~$118M total raised); no newer raise surfaced as of the 2026-06-16 currency scan. Hunters newsroom, accessed 2026-06-16. https://www.hunters.security/newsroom/hunters-secures-68-million-in-series-c-funding-to-become-a-leading-security-operations-platform-1 ↩

71. Dropzone AI raised $37M Series B (2025-07-17, led by Theory Ventures); ~100+ customers; AI Threat Hunter and AI Threat Intel Analyst agents launching Q2 2026, expanding from triage to full-spectrum detection/response. Dropzone press release, accessed 2026-06-16. https://www.dropzone.ai/press-release/dropzone-ai-37m-series-b-funding-ai-soc-agents ↩

72. Vectra AI acquired Netography (cloud-native network observability, terms undisclosed) and was named a Leader in the 2026 Gartner Magic Quadrant for NDR for the second consecutive year. SecurityBuzz, accessed 2026-06-16. https://securitybuzz.com/industry-news/vectra-ais-netography-acquisition-marks-a-new-era-for-ai-driven-network-defense/ ↩

73. SentinelOne (NYSE: S) investor relations — quarterly earnings transcripts and 10-Q filings disclosing non-endpoint ARR mix. SEC EDGAR, accessed 2026-06-16. https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=0001583708 ↩

74. Microsoft Sentinel/Defender transition timeline and unified-SOC-plane framing. Microsoft Tech Community, accessed 2026-06-16. https://techcommunity.microsoft.com/blog/microsoftsentinelblog/update-new-timeline-for-transitioning-sentinel-experience-to-defender-portal/4490464 ↩

75. Cisco (NASDAQ: CSCO) security-segment and Splunk-momentum disclosures. Cisco Form 8-K (Q3 FY2026 press release), accessed 2026-06-16. https://www.sec.gov/Archives/edgar/data/0000858877/000085887726000075/exhibit991pressrelease-q3f.htm ↩

76. Dropzone AI agentic-SOC roadmap (AI Threat Hunter / AI Threat Intel Analyst, Q2 2026) as a category GA-milestone marker. Dropzone press release, accessed 2026-06-16. https://www.dropzone.ai/press-release/dropzone-ai-37m-series-b-funding-ai-soc-agents ↩

77. CrowdStrike (NASDAQ: CRWD) Falcon Flex ending-ARR disclosures. CrowdStrike Form 8-K (FY2026), accessed 2026-06-16. https://www.sec.gov/Archives/edgar/data/0001535527/000153552726000007/crwd-20260303xex991.htm ↩

Disclosures

DISCLOSURE.

This is ProductBeacon's independent, impartial market research, based solely on publicly verifiable signals, published on the open web. No vendor sponsors, no paywalled data, no analyst-firm reuse. It reflects ProductBeacon's independent view and is not investment advice. Full independence and sourcing methodology: Methodology →.

AFFILIATION.

By Yohay Etsion, Head of Product (Fractional), AXIA. AXIA is an AI-powered data-security (Insider Risk Management / DLP) company. This analysis is based only on publicly verifiable material.

NOT ADVICE.

This report does not constitute investment, legal, tax, or accounting advice. No claim should be relied upon as the basis for any investment decision. The author holds no trading position in any named public security and is not compensated by any named vendor. Readers who use this report in investment contexts bear sole responsibility for their decisions.