PRODUCTBEACON RESEARCH

ProductBeacon — State of Cyber Security Markets 2026, Front 1: The Insider Risk Front

Yohay Etsion

Managing Director, ProductBeacon

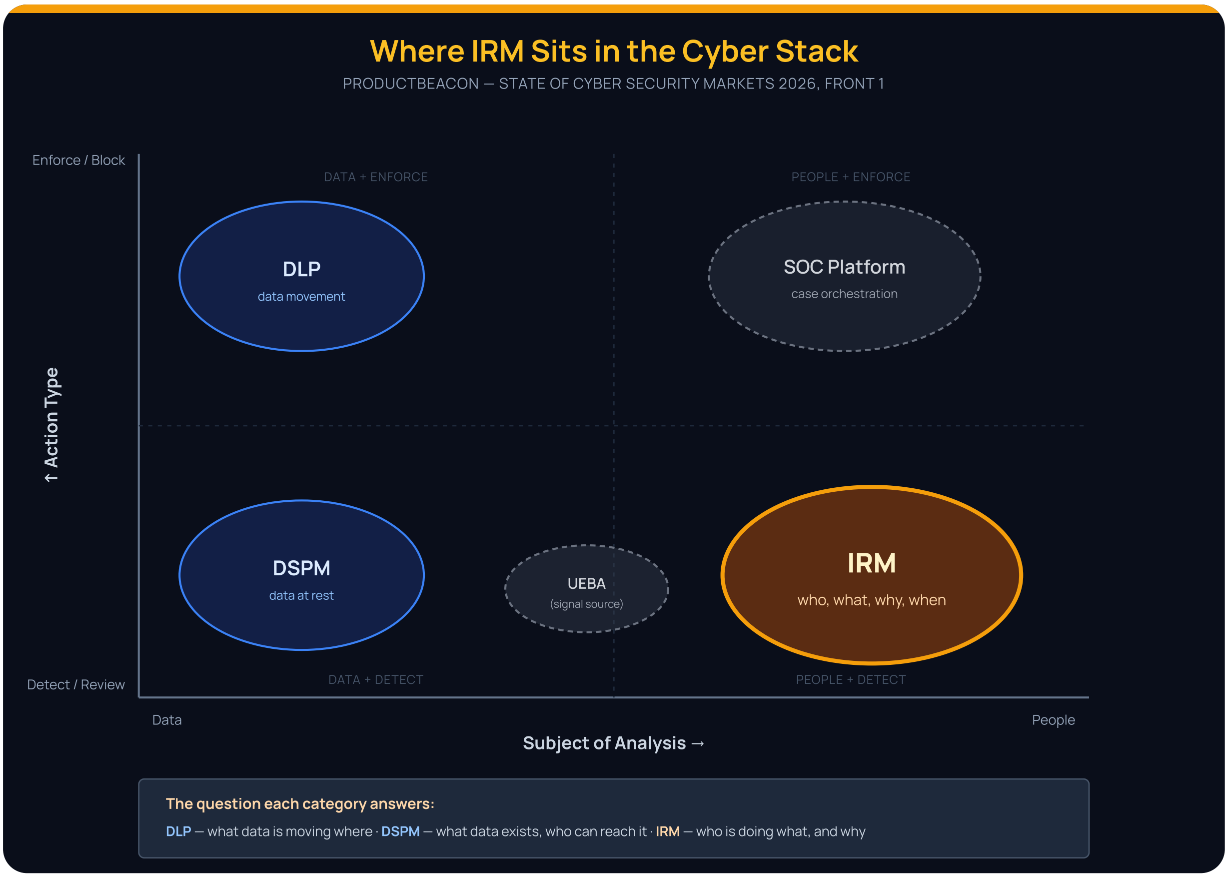
June 2026

ProductBeacon — State of Cyber Security Markets 2026, Front 1: The Insider Risk Front

1.1 The Playing Ground

Insider Risk Management (IRM) is the discipline of detecting, investigating, and acting on risks created by people inside an organization who have legitimate access to data, systems, and decisions. The buyer noun is *people* — who, what, why, when — not data flows (DLP) or data at rest (DSPM). The architectural anchor is behavioral and contextual analysis of signals ingested from communication, file, identity, and endpoint surfaces, then scored against role-baselines and policy templates that produce alerts a human reviewer triages into cases.

Where the categories overlap. IRM overlaps with DLP on context-aware enforcement, with DSPM on access-pattern visibility, and with SOC platforms on case orchestration. The category test is which question a vendor's product actually answers: IRM answers *who is doing what, and why*; DLP answers *what data is moving where*; DSPM answers *what data exists, and who can reach it*. When a vendor's hero page claims all three, the practical test is which question their pricing, sales motion, and alert experience are actually built around.



Where IRM Sits in the Cyber Stack — IRM, DLP, DSPM, UEBA, and SOC platforms positioned by Subject of Analysis × Action Type

The IRM category sits in the people / detect-and-review quadrant. DLP and DSPM share the data side; SOC platforms sit above as cross-domain case orchestrators. UEBA is a signal source to IRM, not a peer category.

What IRM IS. A behavioral and policy-driven workflow for risks where a known identity does a thing — exfil before resignation, sharing IP with a personal account, abnormal access to a sensitive folder, prompt-injecting sensitive content into a public LLM, escalating privilege without ticketed justification. It is policy-template driven (departing-user template, priority-user template, AI-usage template) and produces case files reviewers work in collaboration with HR and Legal.

What IRM IS NOT. Not a SIEM (correlates external threats too), not a DLP (here, enforcement is human-reviewer notification or HR escalation, not inline block), not a UEBA tool alone (those are an input signal, not the workflow), and not a SOAR (the playbooks here cross HR and Legal, not just SecOps).

Three common buyer misconceptions. First: "we already have DLP, we don't need IRM." DLP fires on data movement; IRM fires on a person's risk trajectory across many movements and signals, including ones DLP doesn't see. Second: "IRM is just employee monitoring with extra steps." The privacy-by-design posture of the modern category

(Microsoft Purview pseudonymizes by default per its product docs [1]; DTEX cites a "privacy-first" architecture [2]) is the difference between IRM and 2010s surveillance tooling. Third: "AI agents aren't insiders." Above Security's funding thesis (March 2026, $50M Series A [3]) and Microsoft Purview's new "Risky Agents" policy template [4] both treat non-human identities as in-scope; this is becoming consensus.

1.2 The Terrain

Market sizing. Two estimates worth naming side-by-side, not averaged: Custom Market Insights projects $4.5B in 2026 with a 12.6% CAGR through 2035 [5]; Future Market Insights projects $3.2B in 2025 growing to $10.3B by 2035 at 12.5% CAGR [6]. Both sources are private firms and not endorsed by Gartner or IDC; the 2026 Gartner Market Guide for IRM Solutions (the most-cited primary analyst document in vendor marketing) does not publish a sizing number in the publicly accessible material [7]. The takeaway is not a precise number — it is that two independent forecasters land within ~30% of each other in the same year, and both project a sustained low-teens CAGR. The market is mid-sized, growing steadily, and consolidating buyers who previously held DLP and IRM as separate line items.

Buyer trends. Three signals shape the 2026 buyer. First, the CISO consolidation push: the buyer increasingly evaluates IRM as a *module of* a broader data-security or human-risk platform, not as a standalone PO. Mimecast's acquisition of Code42 (July 2024 [8]) and Proofpoint's positioning of ITM inside its email/data platform [9] both indicate this. Second, the AI-usage policy template has become table-stakes — Microsoft Purview has shipped both "Risky AI usage" and "Risky Agents (preview)" templates [4]; Cyberhaven, DTEX, and Above all lead with AI-actor framing in their 2026 messaging [10] [2] [3]. Third, privacy-by-design is no longer a differentiator — it is a deal-disqualifier if absent, particularly for EU buyers under GDPR and (increasingly) the EU AI Act.

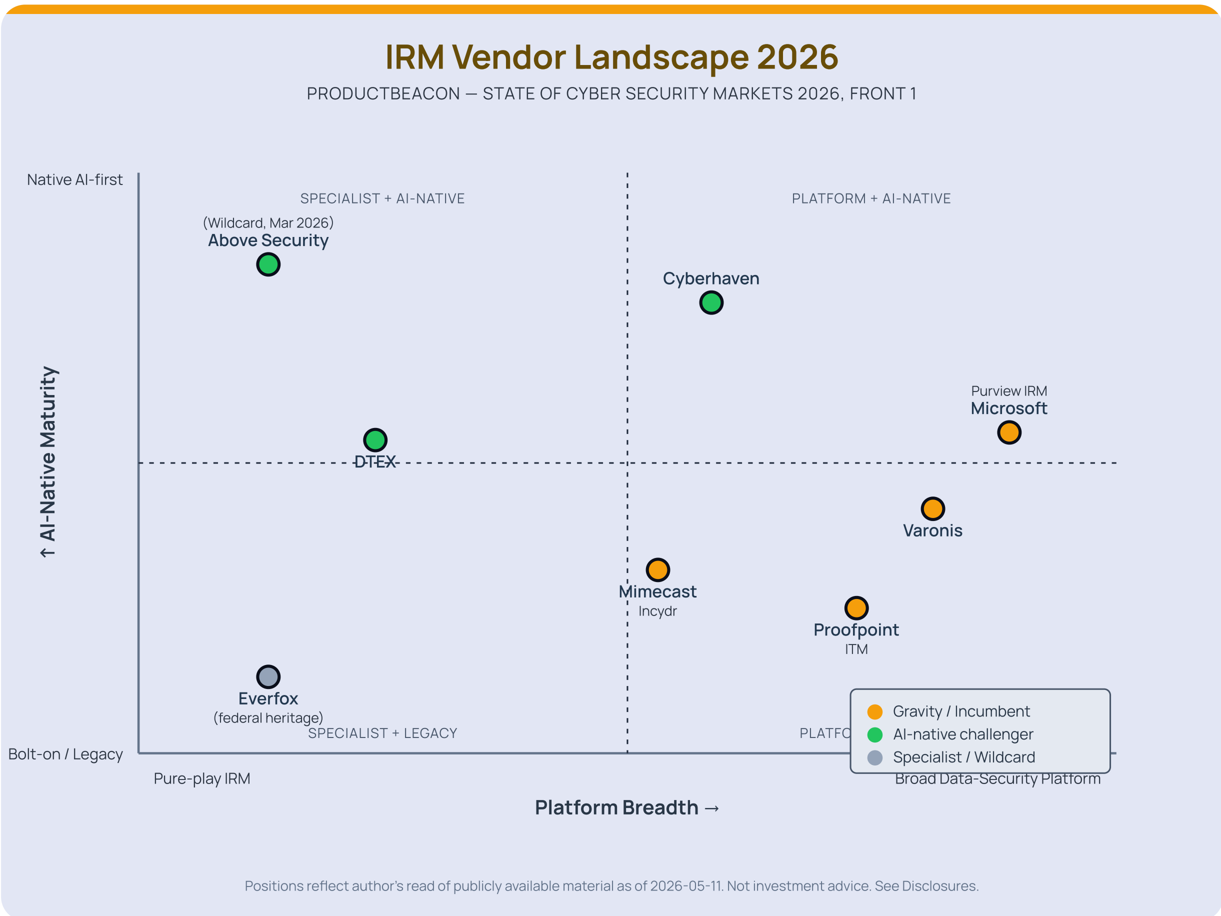
User trends. The end-user experience IRM tools touch has bifurcated. Reviewers (SOC analysts plus HR partners plus Legal counsel) want a single case file with the *narrative* of risk — what happened, in what order, with what context — not a stream of disconnected alerts. The "Triage Agent" UX in Microsoft Purview [4] and the "Linea AI Analyst Agent" autonomous-investigation pattern in Cyberhaven [10] are both responses to alert-fatigue at the reviewer tier.

Tech trends. Behavioral analysis engines have shifted from rule-and-anomaly architectures to LLM-driven semantic understanding of content (Cyberhaven Large Lineage Models [10]; DTEX behavioral intelligence engine [2]; Above's "thousands of AI agents" model [3]). The shared technical claim is that LLMs reduce false positives by understanding *what the content is and why the user touched it*, not just *that a file moved*. Whether this delivers the 90%-FP-reduction numbers some vendors quote in practice is a separate question; the architecture shift is real.

Regulatory trends. Three items shape 2026: EU AI Act enforcement on high-risk automated decision systems (in scope where IRM scores influence HR action); HIPAA / HITECH templates for healthcare insider risk (Microsoft Purview's "Patient data misuse (preview)" template [4]); and the maturation of insider-threat reporting expectations for US federal contractors via NITTF / E.O. 13587 lineage, which is where Everfox's heritage sits.

1.3 The Contenders

Eight vendors selected for this chapter, distributed across three tiers: 3 Gravity (public or post-$100M private), 4 Attention (analyst-mentioned, growing), and 1 Wildcard (seed or early Series A).



IRM Vendor Landscape 2026 — 8 vendors plotted on Platform Breadth × AI-Native Maturity axes

Author's read of public material, May 2026. Vendor positions are conceptual, not data-derived. Color-coding by tier: amber for Gravity (incumbents), green for AI-native *challengers, grey for specialists and Wildcards. Not investment advice.*

Gravity tier

Microsoft Purview Insider Risk Management

> *"Microsoft Purview Insider Risk Management is a compliance solution that helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization." — Microsoft Learn product docs, accessed 2026-05-11* [11]

Purview IRM is the volume leader by distribution reach. Distribution is bundled inside Microsoft 365 E5 and Purview SKUs; the buyer rarely makes a standalone IRM purchase decision — IRM activates as part of a broader Purview rollout. Stated USP is the breadth of Microsoft 365 + Graph signal coverage and a library of pre-built policy templates (twelve listed in current docs including "Data theft by departing users," "Risky AI usage," and "Risky Agents (preview)" [11]). Target buyer is the CISO at a Microsoft-standard enterprise, with the actual purchasing motion routed through the M365 contract. Pricing signal: bundled inside E5 + per-user Purview add-on; not separately listed. Architectural classification: cloud-native, signal-rich, Microsoft-tenant-bounded. Published-material tier: heavy — product docs, Mechanics videos, Gartner Peer Insights presence, PwC co-published rollout playbook [11] .

Varonis

> *"Confidently adopt AI, reduce data exposure, and stop AI-powered threats, automatically." — Varonis homepage, accessed 2026-05-11* [12]

Varonis is the publicly-traded data-security veteran (NASDAQ: VRNS) whose insider-risk capability ships inside its Data Security Platform and its Managed Data Detection and Response (MDDR) service. Q4 2025 results: total ARR $745.4M up 16% YoY; SaaS ARR $638.5M (86% of total ARR), 32% YoY growth excluding conversions [13] . The IRM message lives under the wider "data security" umbrella; the company's hero positioning is data and AI security, not insider risk per se. Stated USP is depth of permissions and access-graph telemetry on Microsoft 365, Salesforce, and adjacent SaaS — the "who can access what, and who actually did" data. Target buyer is the enterprise data-security buyer in regulated industries. Pricing signal: subscription per data store, list pricing not public. Architectural classification: SaaS-platform-first as of FY2025 transition; hybrid deployment with Azure-hosted analytics plane and customer-side Collectors for on-prem data sources. Published-material tier: heavy — earnings transcripts, S-1 / 10-K disclosure, analyst coverage.

Proofpoint (Insider Threat Management, formerly ObserveIT)

> *"Contain Insider Threats. Proofpoint insider threat management (ITM) provides visibility into risky behavior that leads to business disruption and revenue loss by careless, malicious and compromised users." — Proofpoint ITM product page, accessed 2026-05-11* [14]

Proofpoint acquired ObserveIT in 2019 for $225M, taking ITM private inside the Proofpoint email-security platform; Thoma Bravo subsequently took Proofpoint private in 2021 at $12.3B [15] . As of mid-2026, Proofpoint is publicly signaling IPO intent and has announced a $1B+ acquisition of Hornetsecurity to fuel European scale [16] . ITM positioning inside the Proofpoint platform leads with endpoint visibility and screen-record forensic evidence — the heritage UX from ObserveIT. Stated USP is unified email + endpoint + cloud visibility for user-centric risk. Target buyer is the email-security-led CISO who has standardized on Proofpoint. Pricing signal: per-user, bundled into Proofpoint platform pricing, not public. Architectural classification: hybrid endpoint + cloud, with the heaviest forensic-evidence experience among the Gravity tier. Published-material tier: heavy — press releases, layoff disclosures via named outlets, Thoma Bravo portfolio commentary.

Attention tier

Cyberhaven

> *"Secure Data. Secure AI. Cyberhaven's AI & data security platform unifies DSPM, DLP, Insider Risk, and AI Security to protect data wherever it lives and goes across endpoints, cloud, on-prem, SaaS, and AI tools." — Cyberhaven homepage, accessed 2026-05-11* [17]

Cyberhaven's $100M Series D in April 2025 at $1B valuation [18] crossed the post-$100M-private threshold but the company's positioning and analyst footprint still sit in the Attention tier rather than Gravity — it has not been public-vendor-grade in earnings visibility. The product story is a unified DSPM + DLP + IRM + AI-Security platform, which deliberately blurs the front boundaries this report enforces; for IRM purposes, the IRM module is positioned as the "user behavior signal" layer of the wider data-lineage engine. Stated USP is data lineage — the "where did this data come from, who touched it, where is it going" graph — fed into IRM as the *why* behind a user's actions. Target buyer is the AI-era CISO consolidating multiple data-security line items into one platform. Pricing signal: enterprise subscription, not public. Architectural classification: cloud-analytics, multi-source-collection (endpoints + browser extensions + cloud apps); unified data-lineage engine. Published-material tier: medium — PR Newswire funding announcements, product launch pressers, Latka revenue disclosures ($52.4M FY 2026 [19]).

DTEX Systems

> *"The Unified Platform for Human + Data + AI Risk. Prevent incidents using the industry's most advanced behavioral intelligence engine." — DTEX homepage, accessed 2026-05-11* [20]

DTEX is the AI-era behavioral-intelligence-led IRM contender, anchored by a $50M Series E in March 2024 led by Alphabet's CapitalG at a valuation north of $400M [21] . The InTERCEPT platform claim is that DLP, UBA, and user-activity-monitoring capabilities are consolidated into a single light-weight endpoint footprint. Stated USP is behavioral intelligence sensitivity at the endpoint without traditional UAM's privacy cost. Target buyer is the enterprise CISO with a stated "insider risk" line item and a preference for behavioral telemetry over content-aware DLP. Pricing signal: per-endpoint, not public. Architectural classification: endpoint-led, behavioral-metadata collection (~500 metadata elements per the vendor); cloud-hosted analytics. Published-material tier: medium — BusinessWire funding announcements, Axios coverage, Gartner Market Guide entries.

Mimecast Incydr (formerly Code42 Incydr)

> *"Adaptive data protection for a changing world. Get unmatched protection against shadow AI and the changing world of work. Incydr delivers adaptive data protection for and by AI." — Mimecast Incydr product page, accessed 2026-05-11* [22]

Mimecast acquired Code42 in July 2024 (deal value undisclosed [23]). The code42.com domain now 301-redirects to mimecast.com/products/incydr [24] , a structural signal worth flagging on its own (see the Mimecast Absorption Thesis below). The Incydr product itself was historically positioned as the mid-market "Insider Risk Cloud" pure-play; under Mimecast it now sits inside a broader Human Risk Management positioning that bundles security awareness training, email, and Incydr behavioral signal. Stated USP under the new positioning is "shadow AI" coverage on endpoint and SaaS. Target buyer is the Mimecast-standard mid-enterprise. Pricing signal: bundled inside Mimecast HRM tiers, not public. Architectural classification: endpoint-agent + cloud-SaaS-API; cloud-analytics plane. Published-material tier: medium — Mimecast press releases, named-outlet acquisition coverage (Dark Reading, StarTribune, The Deal).

Everfox (Insider Threat Solutions, formerly Forcepoint Insider Threat)

TPG acquired the Forcepoint Global Governments and Critical Infrastructure (G2CI) business — which contains the Insider Threat / Cross Domain heritage — from Francisco Partners for $2.45B in Q4 2023; the asset was rebranded Everfox in January 2024 [25]. Stated USP is government-grade insider-threat and cross-domain solutions — the NITTF / federal-contractor heritage is the moat, not a side note. Target buyer is the federal civilian, DoD, defense-industrial-base, or government-adjacent regulated enterprise. Pricing signal: enterprise contract, not public. Architectural classification: hybrid on-prem + cloud, government-deployment-hardened. Published-material tier: medium — Washington Technology, GovCon Wire, BusinessWire — federal-trade-press dense, commercial-trade-press thin.

Wildcard tier

Above Security

> *"AI agents are becoming insiders in everything but name." — Aviv Nahum, Co-Founder, quoted in PR Newswire and Ynet News funding coverage, March 2026* [26] [27]

Above Security emerged from stealth in March 2026 with $50M total funding ($7M Seed + ~$43M Series A) led by Ballistic Ventures, Merlin Ventures, and Norwest, with Jump Capital and QPV participating [26]. Founders are Aviv Nahum (Unit 81 alum) and Amir Boldo (Unit 49 alum), both Israeli intelligence-veteran lineage. The thesis is that AI agents — non-human identities operating at machine speed across enterprise systems — are insiders in everything but name, and that conventional IRM scoring built around human-baseline behavior misses them entirely. The product claim is rapid deployment "in minutes, without writing a single policy, rule, or configuration" using thousands of AI agents observing both human and machine behavior. Architectural classification: multi-source collection (endpoint + identity + SaaS + AI environments); cloud-hosted AIinvestigator fleet. Published-material tier: Wildcard-level — named-outlet coverage (Calcalist, Ynet, PR Newswire, SecurityMEA, StartupHub.ai, Pulse2, Artiverse) but no analyst coverage, no public reference customers named in primary materials, no public pricing.

1.4 Their Plays

Four strategic moves in motion across 2026.

Play 1: The Unified Data Security Platform Bundle

- **Observation.** Cyberhaven launched a unified DSPM + DLP + IRM + AI-Security platform in February 2026 [28]. Varonis' SaaS ARR transition (86% of ARR by Q4 2025 [13]) and its MDDR + Copilot positioning collapse data classification, access governance, and insider-risk telemetry into one subscribable platform. Microsoft Purview houses IRM inside the broader Purview suite by design.
- **Participants.** Cyberhaven, Varonis, Microsoft.
- **Conditional outcome.** *If the unified-platform pitch displaces standalone IRM line items in 2026 enterprise renewals, the standalone IRM specialists (DTEX, Mimecast Incydr post-absorption, Teramind) face structural buyer-side pressure on renewal pricing. If the platform pitch under-delivers on IRM depth — and reviewer-level UX is the most likely failure mode — specialists retain their lane on the renewal cycle through 2027.*
- **Evidence.** Cyberhaven Fall 2025 product launch page; Varonis Q4 2025 earnings transcript [13].

Play 2: The AI-Actor Insider Framing

- **Observation.** Microsoft Purview shipped "Risky AI usage" and "Risky Agents (preview)" policy templates in 2025-2026 [11]. Above Security's funding thesis explicitly frames AI agents as insiders [26]. Cyberhaven's Linea AI Detection Agent and Linea AI Analyst Agent (announced 2025) reposition the product around AI-native detection and investigation [17] [29]. DTEX's "Human + Data + AI Risk" homepage tagline as of 2026-05-11 places AI on equal footing with the human-risk category [20].
- **Participants.** Microsoft, Above, Cyberhaven, DTEX, and increasingly the entire field.

- **Conditional outcome.** *If by Q4 2026 every Gravity-tier vendor has shipped both an AI-usage detection template and an autonomous-agent-investigation experience, AI-actor framing becomes table stakes — no longer a differentiator. If only a subset does (most likely Microsoft, Varonis, Cyberhaven), the AI-actor framing remains a wedge that the platform-incumbents extract more value from than the specialist tier.*
- **Evidence.** Microsoft Learn policy template list [11] ; Above PR Newswire [26] ; Cyberhaven Linea product page [29] .

Play 3: Federal-Heritage Specialization

- **Observation.** Everfox's January 2024 rebrand from Forcepoint Federal explicitly anchors the asset in defense-grade insider-threat and cross-domain solutions [25] ; Everfox subsequently acquired Garrison Technology in June 2024 [30] . The federal insider-threat program lineage (NITTF / E.O. 13587) is a different buying motion from commercial IRM.
- **Participants.** Everfox, with quieter federal exposure from Microsoft (FedRAMP-authorized Purview) and Proofpoint (FedRAMP-authorized email/ITM).
- **Conditional outcome.** *If federal IRM spend continues to grow at the regulatory-driven rate signaled by 2024-2025 budget activity, Everfox's specialist position is structurally protected and the commercial-side IRM platforms cannot economically pursue the same buyer. If federal procurement reorients toward "approved commercial platform" preferences (Microsoft, Proofpoint), Everfox's moat narrows to cross-domain solutions specifically, with the broader insider-threat capability becoming a commercial-platform feature.*
- **Evidence.** Washington Technology January 2024 [25] ; BusinessWire June 2024 Garrison announcement [30] .

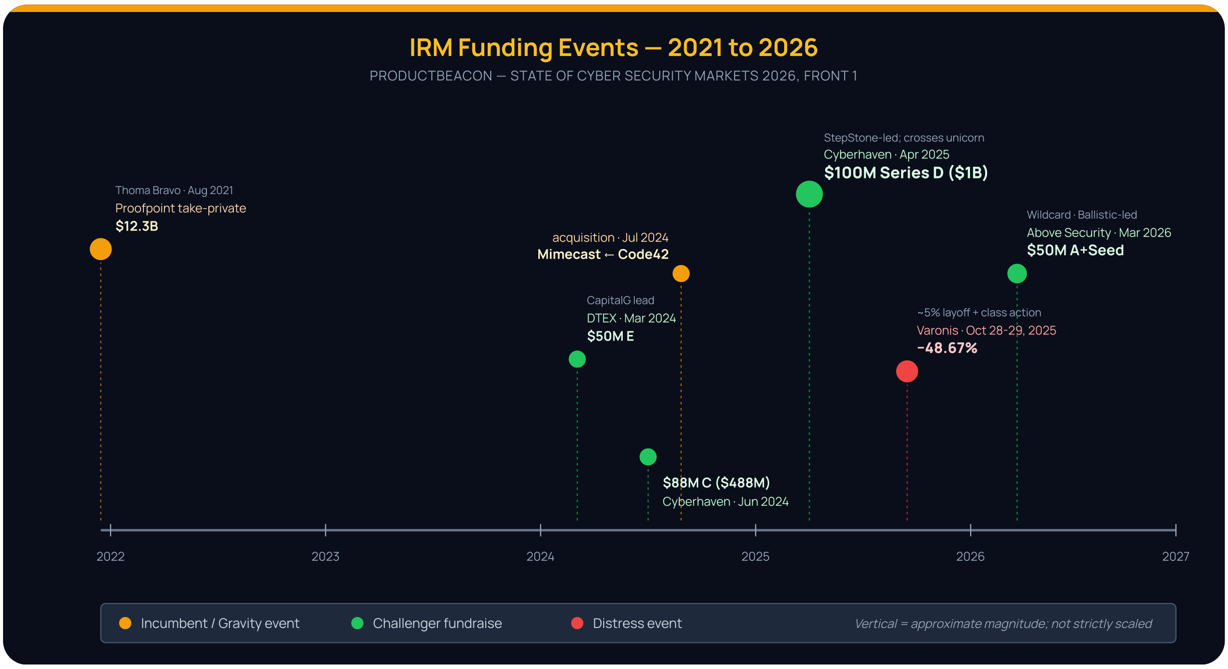
Play 4: The Proofpoint IPO Re-Entry

- **Observation.** Proofpoint announced a $1B+ acquisition of Hornetsecurity in May 2025 framed by CNBC as IPO-prep [16] . Proofpoint's CEO publicly signaled return-to-public-markets intent in 2026 [16] . ITM sits inside the Proofpoint platform that would re-IPO.
- **Participants.** Proofpoint, Thoma Bravo, potential 2026 IPO market window.

- **Conditional outcome.** *If Proofpoint re-IPOs in 2026 with ITM as a named segment, the public-market disclosure cadence raises the analytic visibility of the entire IRM category — earnings transcripts and 10-K segment reporting become a new IRM benchmark alongside Varonis. If the IPO slips to 2027 or the platform is sold rather than IPO'd, ITM remains a sub-line in private-company press cycle.*
- **Evidence.** CNBC May 2025 [16] ; Thoma Bravo portfolio commentary [31] .

1.5 War Chests & Casualties

Snapshot of recent funding events, valuations, strategic investors, and any documented distress signals across the IRM front. All figures trace to vendor-controlled surfaces, SEC filings, or named-outlet journalism (TechCrunch, Reuters, Bloomberg, Calcalist, BusinessWire, SecurityWeek, PR Newswire, GlobeNewswire). Executive departures appear only when corroborated by two or more named outlets; LinkedIn-only signals are treated as positioning facts, not distress events.



IRM Funding Events — 2021 to 2026, by date, magnitude, and event type

A five-year compression of the IRM money story: Thoma Bravo's $12.3B take-private of Proofpoint in 2021; the late-stage round cluster across DTEX, Cyberhaven, and Mimecast/Code42 in 2024; Cyberhaven crossing $1B in April 2025; the Varonis re-rating in October 2025; and Above Security closing the most recent round, at $50M, in March 2026.

VENDOR	MOST RECENT ROUND	VALUATION (IF PUBLIC)	STRATEGIC INVESTOR	DISTRESS SIGNAL
Microsoft (Purview IRM module within M365 E5 / E5 Compliance) [32]	n/a — bundled within M365 E5 licensing [33]	Public parent (NASDAQ: MSFT); IRM revenue not broken out separately	n/a — platform bundling	—
Varonis Systems (NASDAQ: VRNS)	Public — Q4 2025 results released Feb 3, 2026 (EPS \$0.08 beat vs. –\$0.07 consensus; Q4 revenue \$173M, +9% YoY) [34]	Market cap fell below \$4B following Oct 28, 2025 disclosure (down 48.67% intraday from \$63.00 to \$32.34 on Oct 29, 2025) [35]	n/a — public company	**~5% workforce layoff announced alongside Q3 2025 results; securities class action filed Jan 2026 (Hagens Berman, Berger Montague, ZLK) alleging misrepresentation of on-prem-to-SaaS conversion trends during the class period Feb 4 – Oct 28, 2025** [36] [37]
Proofpoint (private; ITM via ex-ObserveIT acquisition)	Thoma Bravo take-private closed Aug 31, 2021 at \$176.00/share cash, ~\$12.3B transaction value [38] [39]	Thoma Bravo (PE sponsor)	— *(enterprise-level layoffs noted in Watch below; no ITM-specific casualty event)*	
Cyberhaven (data-lineage IRM/DLP-adjacent)	Series D — \$100M led by StepStone Group (Schroders, Industry Ventures participating), announced Apr 2, 2025; total funding \$250M [40] [41]	StepStone Group (NASDAQ: STEP); priors: Adams Street, Khosla, Redpoint, Costanoa, Vertex, Wing	\$1B post-money valuation (≈7× from \$488M Series C in Jun 2024) [42]	—
DTEX Systems (pure-play IRM)	Series E — \$50M led by CapitalG (Alphabet's growth fund), announced Mar 5, 2024;	CapitalG (Alphabet)	\$400M+ post-money valuation per Series E disclosure [45]	—

VENDOR	MOST RECENT ROUND	VALUATION (IF PUBLIC)	STRATEGIC INVESTOR	DISTRESS SIGNAL
	cumulative funding $138M [43] [44]			
Above Security (Wildcard; AI-agents-as-insiders thesis)	$50M total funding ($7M Seed + ~$43M Series A); stealth-exit announced Mar 23, 2026 [26]	Private — not disclosed	Ballistic Ventures (lead), Merlin Ventures, Norwest Venture Partners, with Jump Capital and QPV participating [26]	—

The IRM funding picture splits three ways. **Platform-bundled positioning** — Microsoft Purview included in M365 E5 — competes on attach, not on IRM ARR; revenue is not separately disclosed [32]. The **public pure-play** — Varonis — re-rated sharply on Oct 28, 2025 after disclosing weaker renewals and ARR conversion in its SaaS transition; the 48.67% single-day drop, the ~5% workforce reduction, and the subsequent securities class action collectively anchor the distress label in row 2 — the only such call in this chapter — to specific cited public events [35] [36] [37]. The **VC-funded specialists** — Cyberhaven, DTEX, Above Security — raised at progressively richer terms through 2024 – 2026, with Cyberhaven crossing $1B in Apr 2025 [41] and Above closing the most recent round at $50M in Mar 2026 [26]. CapitalG (DTEX) and StepStone (Cyberhaven) both signal late-stage growth-investor conviction in pure-play IRM despite the Varonis re-rating.

Cross-reference. See the Venture Landscape chapter for deep cross-segment analysis. The Cyberhaven $1B Series D anchors Pattern Claim 2 below — on late-stage growth conviction in pure-play data-lineage IRM.

Not investment advice. See Disclosures.

1.6 Winning & Losing

Three themes shape what's winning and losing in IRM today. Each is anchored to public evidence, framed explicitly as opinion, and stated as a falsifiable prediction that the next twelve months will either confirm or refute.

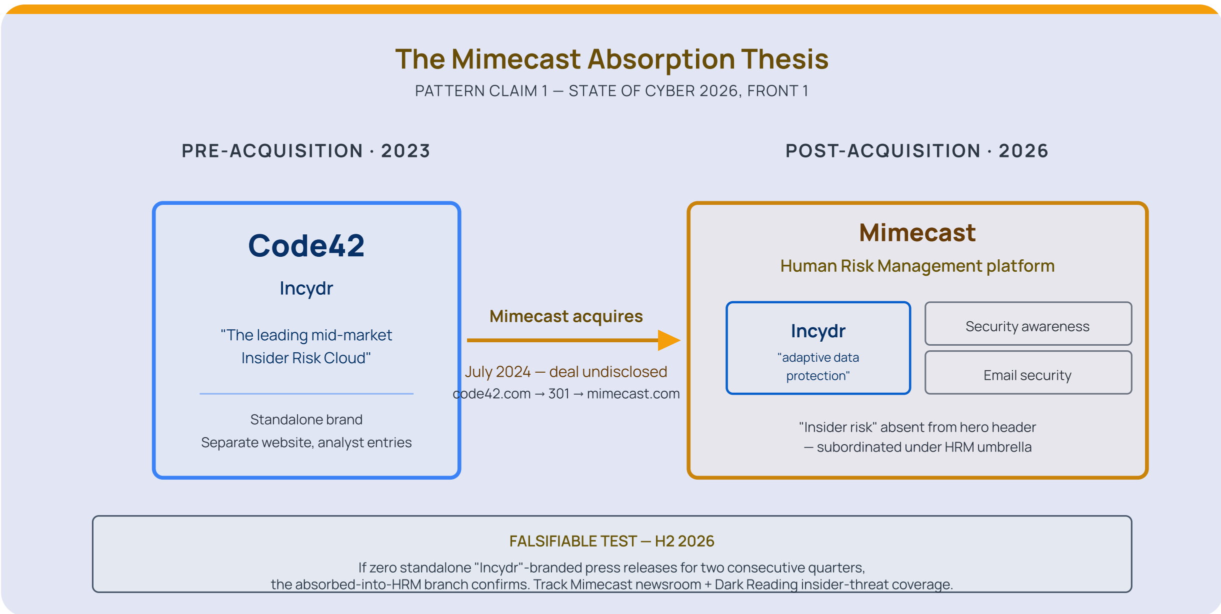
Pattern Claim 1 — The Mimecast Absorption Thesis

Observation. Code42 Incydr, the leading mid-market insider-risk pure-play through 2023, was acquired by Mimecast in July 2024; deal value undisclosed [46]. The code42.com homepage now 301-redirects to mimecast.com/products/incydr [47]. Mimecast's positioning of the asset has shifted from "insider risk management" to "Human Risk Management platform" language; the Incydr page hero now reads "Adaptive data protection for a changing world" with no use of the phrase "insider risk" in the primary header [48].

My read. I read this as Mimecast subordinating the insider-risk category narrative to a broader "human risk" umbrella that bundles security awareness training, email security, and Incydr behavioral signal. The standalone IRM brand is being absorbed, not preserved as a specialist motion. This is consistent with how rollup platforms typically treat a category acquisition once the deal closes — the acquired narrative bends to the parent's positioning.

Conditional prediction. *If Mimecast's H2 2026 product cadence shows Incydr-branded releases on parity with pre-acquisition velocity (benchmarked against Code42's 2022-2023 release-note volume), the absorption is structural-only and the product survives as a recognizable line. If Incydr is described only as a "module" or "capability" of the Mimecast HRM platform by Q4 2026 — no standalone branded release notes, no Incydr-led webinars, no separate analyst entries — the absorption has consumed the standalone identity.*

Sources. [46] [47] [48]



The Mimecast Absorption Thesis — Code42 Incydr standalone brand subordinated under Mimecast's Human Risk Management platform, post-July 2024 acquisition

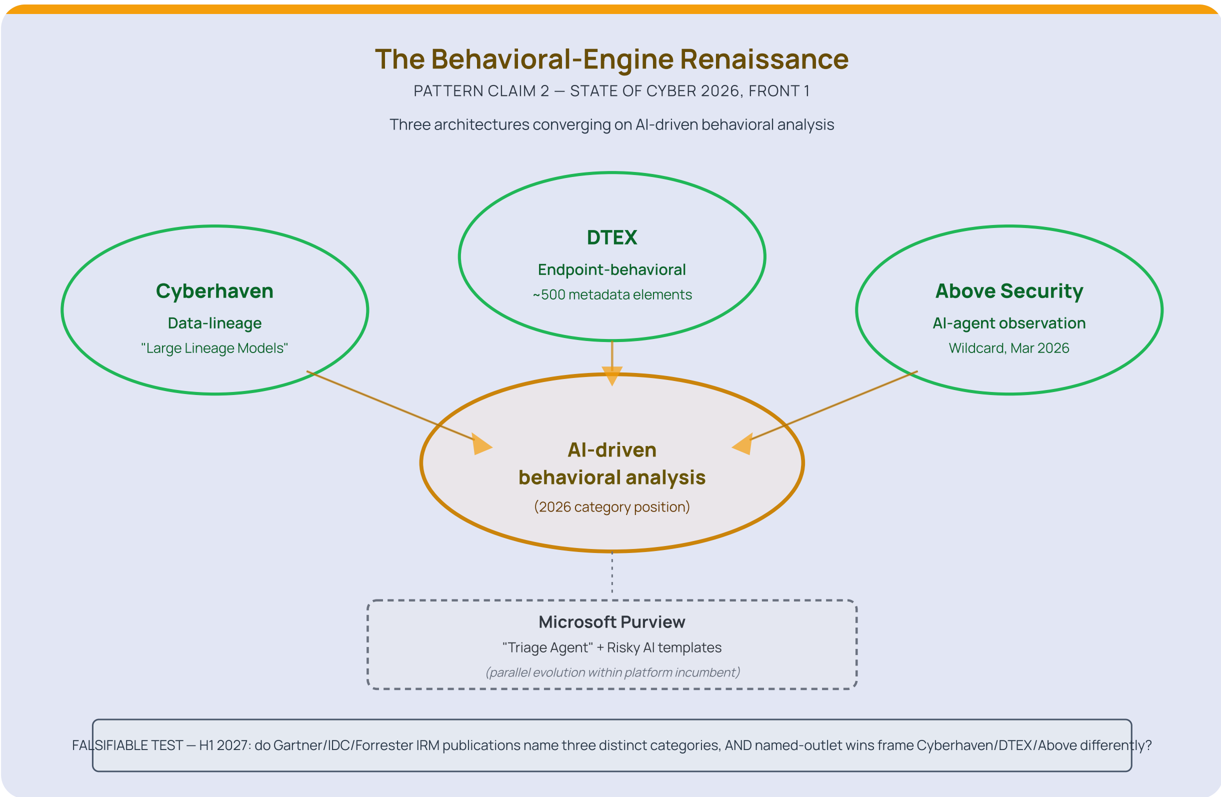
Pattern Claim 2 — The Behavioral-Engine Renaissance

Observation. Three of the eight Contenders are leading their 2026 messaging with a renamed or rearchitected behavioral-engine claim: Cyberhaven's Linea AI Detection Agent and Linea AI Analyst Agent built on "Large Lineage Models" [49] ; DTEX's "industry's most advanced behavioral intelligence engine" anchoring an InTERCEPT product story [50] ; Above Security's "thousands of AI agents" continuous-observation architecture, funded at $50M Series A in March 2026 [51] . Microsoft Purview's "Triage Agent" and policy-template-driven workflow [52] is a parallel evolution within the platform incumbent.

My read. I read this as the IRM category's 2026 product narrative converging on AI-driven behavioral analysis at the *content* and *intent* layer, rather than the rule-and-anomaly layer that defined 2018-2023 UEBA tooling. The shift is real architecture, not pure marketing — the product claims (semantic content understanding, autonomous multi-step investigation) require the long-context LLM models and agent-orchestration tooling that weren't available three years ago. But "behavioral intelligence engine" is also becoming a category-marketing convergence in which every vendor sounds increasingly alike on the homepage, which raises the bar for differentiation in the next renewal cycle.

Conditional prediction. *If by H1 2027 Gartner, IDC, or Forrester IRM coverage (Magic Quadrant, Hype Cycle, MarketScape, Wave) carries distinct named differentiator categories for data-lineage, endpoint-behavioral, and AI-agent-observation approaches — and at least one named-outlet 2026-2027 enterprise reference win for each of Cyberhaven, DTEX, and Above is published with the differentiator-specific framing intact — the renaissance produces three (or more) distinct sustainable positions visible in the public analyst and customer-win record. If analyst reports continue grouping the three under a single "behavioral IRM" or "user activity monitoring" category, and named-outlet customer-win coverage describes them interchangeably, the field collapses toward the Gravity-tier bundled platforms (Microsoft, Varonis) on a price-per-seat basis.*

Sources. [49] [50] [51] [52]



The Behavioral-Engine Renaissance — Cyberhaven (data-lineage), DTEX (endpoint-behavioral), and Above Security (AI-agent observation) converging on AI-driven behavioral analysis

Pattern Claim 3 — The Federal-Heritage Moat

Observation. Everfox emerged in January 2024 from a $2.45B TPG carve-out of the Forcepoint Global Governments and Critical Infrastructure (G2CI) business [53]; the rebrand was explicitly positioned around "defense-grade cybersecurity" with cross-domain solutions and insider-threat solutions as named product lines [53] [54]. The federal insider-threat compliance lineage (NITTF / E.O. 13587 / DoD-specific cleared-personnel requirements) creates a procurement and product-certification path that commercial IRM platforms have not pursued at depth.

My read. I read this as a durable structural moat — not a market-size moat (the federal IRM total addressable market is narrower than commercial) but a defensibility moat. Government buyers are not price-shopping insider-threat tooling against commercial unified-platform pitches; they are evaluating cleared-personnel access, accredited deployment posture, and cross-domain certifications. Microsoft Purview and Proofpoint ITM both have FedRAMP authorizations, but neither leads with federal-mission-specific framing the way Everfox does post-rebrand.

Conditional prediction. *If H2 2026 and 2027 federal procurement maintains its current preference for specialist mission-aligned vendors, Everfox's position holds and the company's commercial expansion (Garrison Technology acquisition June 2024 [55]) is a defensible adjacency. If federal procurement reorients meaningfully toward "approved commercial platform" preferences — and the relevant signal is FedRAMP-High platform displacement of specialist Cross Domain Solutions — Everfox's moat narrows toward cross-domain hardware-software specifically, with broader insider-threat capability migrating to the commercial-platform incumbents.*

Sources. [53] [54] [55]

Winners.

- **Microsoft Purview Insider Risk Management.** Distribution moat via M365 E5 bundling is structural. Policy-template breadth (twelve templates including AI-specific templates [11]) is the broadest in the category by published-material count. The Winners label here is opinion-labeled: I read Microsoft's position as winning the *default-choice* slot in Microsoft-standard enterprises, not winning every IRM deal on technical depth.

- **Varonis.** Public-market discipline (NASDAQ:VRNS, 16% YoY total ARR growth in Q4 2025, 32% SaaS-ARR growth excluding conversions [13]) and a successful SaaS-platform transition position Varonis as the most analyzable winner in the Gravity tier — the one whose performance can be tracked quarter-by-quarter rather than inferred from press cycle.
- **Cyberhaven.** Series D at $1B valuation April 2025 [18], $52.4M revenue [19], unified-platform launch February 2026 [28]: the company has compounded fundraising, revenue, and product-platform position simultaneously in a 14-month window. Winning the *platform consolidation* narrative among Attention-tier vendors.
- **Proofpoint ITM.** A layoff disclosure (280 employees Jan 2024 [56]) is a real signal but it is an enterprise-level Proofpoint cost action, not an ITM-specific casualty event. A casualty label requires the cited event to anchor a vendor-specific decline; what we have anchors enterprise-level cost discipline pre-IPO. Recategorized as Watch accordingly: track whether the H2 2026 IPO filing names ITM as a growth segment or as a maintenance segment.
- **Mimecast Incydr.** See Pattern Claim 1. The Watch signal is release-cadence and analyst-entry preservation through Q4 2026.

No IRM Contender earns a Losers label in this chapter. A vendor reaches this section only when a cited public event — layoff, missed quarter, down-round, named executive departure, or customer-churn disclosure — is specific to that vendor's IRM business, not a parent-company-wide action. As of May 2026, no IRM Contender meets that bar. Proofpoint's enterprise-level layoffs appear in Watch above. Code42's acquisition by Mimecast is restructuring, not a distress event. Quarterly refreshes will populate this section if IRM-specific signals emerge.

1.7 The Campaign Ahead

Five watchlist items for H2 2026.

1. **Proofpoint IPO filing.** Signal to monitor: S-1 filing date and segment reporting structure. Threshold for re-assessment: ITM named as a reportable segment with discrete revenue disclosure → revisit the Winners block above. Primary source: SEC EDGAR; CNBC Cybersecurity vertical.

1. **Mimecast Incydr release cadence.** Signal: Mimecast press-release stream and product-doc release notes through Q3-Q4 2026. Threshold: zero standalone "Incydr" branded press releases for two consecutive quarters → Pattern Claim 1's

"absorbed" branch is realized. Primary source: Mimecast newsroom; Dark Reading insider-threat coverage.

1. **Above Security customer references.** Signal: public reference customers, analyst inclusion in Gartner Market Guide or Hype Cycle, and any expansion-round announcement past Q3 2026. Threshold: named Fortune-1000 reference + analyst inclusion → Above moves from Wildcard to Attention tier in the next refresh. Primary source: PR Newswire; Calcalist; Gartner Peer Insights.

1. **AI-Agent template proliferation.** Signal: which Gravity-tier vendors have shipped an "AI agent monitoring" or "non-human identity insider" capability with a documented detection model. Threshold: by end-2026 if Microsoft Purview and Varonis both have GA capabilities, the AI-actor framing is table-stakes per Pattern Claim 2's first branch. Primary source: vendor docs (Microsoft Learn, Varonis docs); analyst Magic Quadrant updates.

1. **Cyberhaven public-market readiness.** Signal: revenue trajectory disclosures, expansion fundraising rounds, M&A activity (per Cyberhaven's stated 2025 M&A intent [18]). Threshold: ARR disclosure crossing $100M with sustained 80%+ growth → Gravity-tier reclassification in next refresh; alternatively, an acquisition by a Gravity-tier platform → Pattern Claim 1 generalizes to the Attention tier. Primary source: Cyberhaven press releases; PE/strategic-buyer M&A coverage in Reuters, Bloomberg.

Keep reading

Three companion artefacts. Same research, three formats.

NEXT CHAPTER

DLP

Where the data-loss-prevention layer holds, and where it folds into DSPM.

COMPANION

Pre-Call Briefing Pack

Three Pattern Claims and the falsifiable tests behind each.

COMPANION

Report Digest

14-page chapter-by-chapter synthesis of all four fronts.

Read the methodology →

About the author →

References

1. Microsoft Learn, "Learn about Insider Risk Management," accessed 2026-05-11. Pseudonymization-by-default cited under "principles." https://learn.microsoft.com/en-us/purview/insider-risk-management ↩

2. DTEX product page, accessed 2026-05-11. https://www.dtex.ai/ ↩

3. PR Newswire, "Above Security Raises $50M to Solve Insider Risk in the Agentic Era," 2026-03-23. https://www.prnewswire.com/news-releases/above-security-raises-50m-to-solve-insider-risk-in-the-agentic-era-302721984.html ↩

4. Microsoft Learn, Insider Risk Management policy templates list including "Risky Agents (preview)" and "Risky AI usage," accessed 2026-05-11. https://learn.microsoft.com/en-us/purview/insider-risk-management ↩

5. Custom Market Insights, "Global Insider Risk Management (IRM) Market Size 2026-2035," accessed 2026-05-11.

https://www.custommarketinsights.com/report/insider-risk-management-irm-market/ ↩

6. Future Market Insights, "Insider Risk Management Market," accessed 2026-05-11. https://www.futuremarketinsights.com/reports/inside-risk-management-market ↩

7. Gartner, "Market Guide for Insider Risk Management Solutions," 2026, document referenced in vendor marketing materials. Cited via DTEX republication: https://www.dtex.ai/blog/gartner-market-guide-takeaways/ ↩

8. Mimecast Press Release, 2024-07-24. https://www.mimecast.com/resources/press-releases/mimecast-announces-acquisition-of-code42/ ↩

9. Proofpoint Insider Threat Management product page, accessed 2026-05-11. https://www.proofpoint.com/us/products/insider-threat-management ↩

10. Cyberhaven Press Release, "Cyberhaven Launches Unified AI & Data Security Platform with DSPM," 2026-02, and Linea product page, accessed 2026-05-11. https://www.cyberhaven.com/product/linea ↩

11. Microsoft Learn, "Learn about Insider Risk Management," accessed 2026-05-11. https://learn.microsoft.com/en-us/purview/insider-risk-management ↩

12. Varonis homepage, accessed 2026-05-11. https://www.varonis.com/ ↩

13. Stock Titan, "Varonis Q4 2025 results: SaaS ARR jumps 88%," 2026-02.

https://www.stocktitan.net/news/VRNS/varonis-announces-fourth-quarter-2025-and-full-year-2025-financial-70v7b04bguy9.html ↩

14. Proofpoint Insider Threat Management product page, accessed 2026-05-11. https://www.proofpoint.com/us/products/insider-threat-management ↩

15. Thoma Bravo Press Release, "Thoma Bravo Completes Acquisition of Proofpoint," August 2021. https://www.thomabravo.com/press-releases/thoma-bravo-completes-acquisition-of-proofpoint ↩

16. CNBC, "Cybersecurity firm Proofpoint to buy European rival for over $1 billion as it eyes IPO," 2025-05-15. https://www.cnbc.com/2025/05/15/cyber-firm-proofpoint-to-buy-europes-hornetsecurity-as-it-eyes-ipo.html ↩

17. Cyberhaven homepage, accessed 2026-05-11. https://www.cyberhaven.com/ ↩

18. PR Newswire / Cyberhaven Press Release, "Cyberhaven Raises $100 Million Series D at $1 Billion Valuation," 2025-04-02. https://www.prnewswire.com/news-releases/cyberhaven-raises-100-million-series-d-at-1-billion-valuation-302418497.html ↩

19. Latka, Cyberhaven revenue and team size profile, accessed 2026-05-11. https://getlatka.com/companies/cyberhaven.com ↩

20. DTEX homepage, accessed 2026-05-11. https://www.dtex.ai/ ↩

21. BusinessWire, "DTEX Systems Raises $50M Led by Alphabet's CapitalG," 2024-03-04. https://www.businesswire.com/news/home/20240304157963

/en/DTEX-Systems-Raises-$50M-Led-by-Alphabets-CapitalG-to-Disrupt-Insider-Risk-Management-Market-Through-AI-Enabled-Innovations . Valuation per Axios coverage 2024-03-05: https://www.axios.com/2024/03/05/alphabet-dtex-venture-funding-cybersecurity ↩

22. Mimecast Incydr product page, accessed 2026-05-11. https://www.mimecast.com/products/incydr/ ↩

23. Globe Newswire, "Mimecast Announces Acquisition of Code42," 2024-07-24. https://www.globenewswire.com/news-release/2024/07/24/2918058/0/en/Mimecast-Announces-Acquisition-of-Code42-Expands-Human-Risk-Management-Platform-with-Visibility-into-Insider-Threats.html ↩

24. 301 redirect from code42.com → mimecast.com/products/incydr confirmed by direct fetch 2026-05-11. ↩

25. Washington Technology, "The former Forcepoint Federal takes on new name," January 2024. https://www.washingtontechnology.com/companies/2024/01/former-forcepoint-federal-takes-new-name/393722/ . TPG acquisition closing per Forcepoint Newsroom, 2023: https://www.forcepoint.com/newsroom/2023/tpg-completes-acquisition-forcepoint-global-governments-and-critical-infrastructure ↩

26. PR Newswire, "Above Security Raises $50M to Solve Insider Risk in the Agentic Era," 2026-03-23. https://www.prnewswire.com/news-releases/above-security-raises-50m-to-solve-insider-risk-in-the-agentic-era-302721984.html ↩

27. Ynet News, "AI startup Above Security raises $50 million to tackle insider threats as AI agents expand risk," 2026-03. https://www.ynetnews.com/business/article/r1e1xl1swg ↩

28. Cyberhaven Press Release, "Cyberhaven Launches Unified AI & Data Security Platform with DSPM," February 2026. https://www.cyberhaven.com/press-releases/cyberhaven-launches-unified-ai-data-security-platform-dspm ↩

29. Cyberhaven Linea product page, accessed 2026-05-11. https://www.cyberhaven.com/product/linea ↩

30. BusinessWire, "Everfox to Purchase Garrison Technology Ltd," 2024-06-12. https://www.businesswire.com/news/home/20240612545946/en/Everfox-to-Purchase-Garrison-Technology-Ltd-and-Expand-its-Mission-to-Reflect-a-New-Era-of-Defense-Grade-Cybersecurity ↩

31. Thoma Bravo, Proofpoint portfolio page. https://www.thomabravo.com/portfolio/proofpoint ↩

32. Microsoft Learn, *Plan for Insider Risk Management*, https://learn.microsoft.com/en-us/purview/insider-risk-management-plan, accessed 2026-05-11. ↩

33. Microsoft, *Microsoft Purview Suite Pricing*, https://www.microsoft.com/en-us/security/business/purview-suite-pricing, accessed 2026-05-11. ↩

34. The Motley Fool, *Varonis (VRNS) Q4 2025 Earnings Call Transcript*, Feb 3, 2026, https://www.fool.com/earnings/call-transcripts/2026/02/03/varonis-vrns-q4-2025-earnings-call-transcript/. ↩

35. Calcalist Tech, *Varonis shares plunge 45% after surprise earnings miss*, https://www.calcalistech.com/ctechnews/article/h1dc8p1kzl. Hagens Berman / PRNewswire, *Varonis Systems (VRNS) Hit with Securities Class Action*,

https://www.prnewswire.com/news-releases/varonis-systems-inc-vrns-hit-with-securities-class-action-amid-renewal-and-arr-concerns-that-drove-shares-down-48--hagens-berman-302671885.html. ↩

36. Calcalist Tech, *Varonis shares plunge 45% after surprise earnings miss*, https://www.calcalistech.com/ctechnews/article/h1dc8p1kzl ("the company announced plans for staff cuts... laying off around 5% of its workforce"). ↩

37. Berger Montague, *Varonis Systems Securities Fraud Class Action*, https://bergermontague.com/cases/varonis-systems/. ZLK, *Varonis Systems (VRNS) Securities Class Action Lawsuit Filed [Jan 8, 2026]*, https://zlk.com/cases/varonis-systems-inc-class-action-lawsuit-vrns. ↩

38. Proofpoint, *Thoma Bravo Completes Acquisition of Proofpoint*, Aug 31, 2021, https://www.proofpoint.com/us/newsroom/press-releases/thoma-bravo-completes-acquisition-proofpoint. ↩

39. CNBC, *Thoma Bravo's $12.3 billion purchase of Proofpoint is the largest private equity cloud deal*, Apr 26, 2021, https://www.cnbc.com/2021/04/26/thoma-bravo-purchase-of-proofpoint-marks-top-private-equity-cloud-deal.html. ↩

40. SecurityWeek, *Cyberhaven Banks $100 Million in Series D, Valuation Hits $1 Billion*, Apr 2, 2025, https://www.securityweek.com/cyberhaven-banks-100-million-in-series-d-valuation-hits-1-billion/. ↩

41. PRNewswire, *Cyberhaven Raises $100 Million Series D at $1 Billion Valuation*, Apr 2, 2025, https://www.prnewswire.com/news-releases/cyberhaven-

raises-100-million-series-d-at-1-billion-valuation-302418497.html. ↩

42. SecurityWeek, *Data Security Firm Cyberhaven Raises $88 Million at $488 Million Valuation*, Jun 2024, https://www.securityweek.com/data-security-firm-cyberhaven-raises-88-million-at-488-million-valuation/. ↩

43. BusinessWire, *DTEX Systems Raises $50M Led by Alphabet's CapitalG*, Mar 5, 2024, https://www.businesswire.com/news/home/20240304157963/en/DTEX-Systems-Raises-$50M-Led-by-Alphabets-CapitalG-to-Disrupt-Insider-Risk-Management-Market-Through-AI-Enabled-Innovations. ↩

44. Axios, *Alphabet's CapitalG invests $50M in insider risk company Dtex*, Mar 5, 2024, https://www.axios.com/2024/03/05/alphabet-dtex-venture-funding-cybersecurity. ↩

45. FinSMEs, *DTEX Systems Raises $50M in Series E Funding*, Mar 2024, https://www.finsmes.com/2024/03/dtex-systems-raises-50m-in-funding.html ("now valued at more than $400 million"). ↩

46. Mimecast Press Release, "Mimecast Announces Acquisition of Code42," 2024-07-24. https://www.mimecast.com/resources/press-releases/mimecast-announces-acquisition-of-code42/ ↩

47. 301 redirect confirmed via direct fetch 2026-05-11. code42.com → mimecast.com/products/incydr. ↩

48. Mimecast Incydr product page, accessed 2026-05-11. https://www.mimecast.com/products/incydr/ ↩

49. Cyberhaven Linea product page, accessed 2026-05-11. https://www.cyberhaven.com/product/linea ↩

50. DTEX homepage, accessed 2026-05-11.
https://www.dtex.ai/ ↩

51. PR Newswire, "Above Security Raises $50M to Solve Insider Risk in the Agentic Era," 2026-03-23.
https://www.prnewswire.com/news-releases/above-security-raises-50m-to-solve-insider-risk-in-the-agentic-era-302721984.html ↩

52. Microsoft Learn, Insider Risk Management documentation, accessed 2026-05-11.
https://learn.microsoft.com/en-us/purview/insider-risk-management ↩

53. Washington Technology, "The former Forcepoint Federal takes on new name," January 2024.
https://www.washingtontechnology.com/companies/2024/01/former-forcepoint-federal-takes-new-name/393722/ ↩

54. GovCon Wire, "Forcepoint Federal Changes Name to Everfox," 2024-01 (URL re-verified 2026-05-20).
https://www.govconwire.com/articles/forcepoint-federal-changes-name-to-everfox ↩

55. BusinessWire, Everfox Garrison Technology acquisition, 2024-06-12.
https://www.businesswire.com/news/home/20240612545946/en/Everfox-to-Purchase-Garrison-Technology-Ltd-and-Expand-its-Mission-to-Reflect-a-New-Era-of-Defense-Grade-Cybersecurity ↩

56. TechCrunch, "Security giant Proofpoint is laying off 280 employees, about 6% of its workforce," 2024-01-31.
https://techcrunch.com/2024/01/31/proofpoint-layoffs-280-employees/ ↩

•. Everfox Insider Risk Solutions page, accessed 2026-05-11 (URL re-verified 2026-05-20).

https://www.everfox.com/products/insider-risk-solutions — direct fetch returned page-title and navigation only; verbatim hero pillar not extractable at access time. §3.2a escape clause invoked for this row. ↩

- Teramind homepage, accessed 2026-05-11. https://www.teramind.co/ ↩

- Public sources are mixed on Teramind funding history; primary public-source guidance limited to PitchBook, Tracxn, Latka, vendor materials. https://www.crunchbase.com/organization/teramind-inc ↩

- Latka, Teramind profile, accessed 2026-05-11. https://getlatka.com/companies/teramind.co ↩

Disclosures

DISCLOSURE

Disclosure: The author is Head of Product (Fractional) at AXIA, which competes in the Data Loss Prevention segment, adjacent to but not within Insider Risk Management. This chapter uses only publicly available material and reflects the author's personal view, not AXIA's position.

NOT INVESTMENT ADVICE

This report does not constitute investment, legal, tax, or accounting advice. No claim in this report should be relied upon as the basis for any investment decision. The author has 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.