PRODUCTBEACON RESEARCH

ProductBeacon — State of Cyber Security Markets 2026, Front 2: The Data Loss Front

Yohay Etsion

Managing Director, ProductBeacon

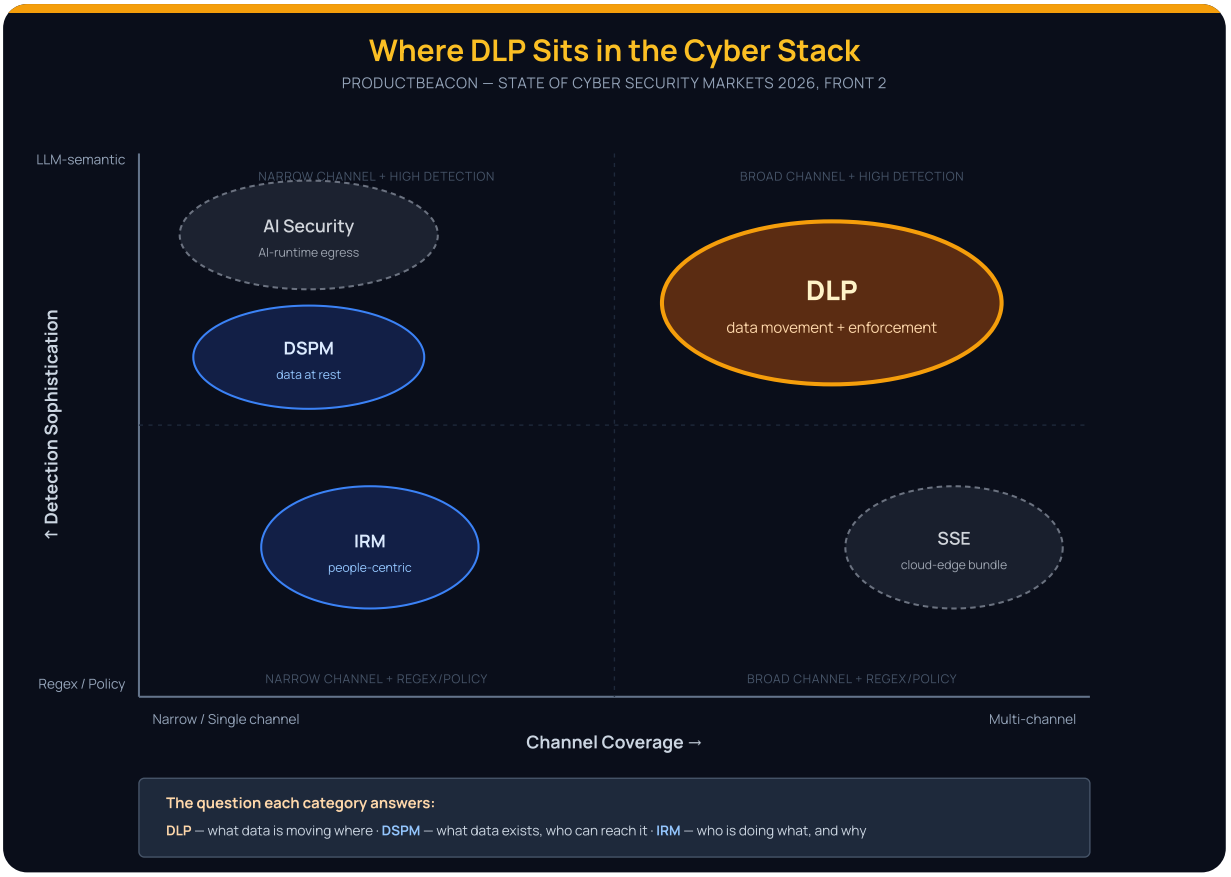
June 2026

ProductBeacon — State of Cyber Security Markets 2026, Front 2: The Data Loss Front

2.1 The Playing Ground

Data Loss Prevention (DLP) is the discipline of detecting, classifying, and acting on sensitive data in motion as it crosses an enforcement boundary — endpoint, network egress, SaaS API, browser session, or, increasingly, the prompt-and-response surface of an AI runtime. The buyer noun is *data flows* — what is moving, of what classification, to where, via which channel — not people (IRM) or data at rest (DSPM). The architectural anchor is a classification engine paired with one or more enforcement primitives (block, encrypt, watermark, quarantine, alert-only), wired into channels the buyer cares about [1] [2]. The 2026 product narrative has shifted from regex-and-fingerprint pattern matching as the *primary* substrate toward AI-classifier substrates — LLM-driven semantic models, ML-trained file classifiers, vendor-proprietary "Large Lineage Model"-style engines, and computer-vision classifiers — and from "stop the file from leaving" toward "stop the sensitive content from being typed into a chatbot or pasted into an agent's tool call" [3] [4] [5]. Incumbents are stacking AI-classifier modules onto their heritage classification pipelines [2] [6]; AI-native entrants ship AI-classifier substrates as the primary detection engine [3] [4].

Where the categories overlap. DLP overlaps with IRM on user-context-aware enforcement, with DSPM on data classification, and with SSE on cloud-edge enforcement. Per the report's taxonomy [7], DLP owns the *data movement* primitive — channel coverage and enforcement primitives — while IRM owns the *people* primitive and DSPM owns the *discovery* primitive. The category test is which question a vendor's product actually answers: DLP answers *what data is moving where, and should we stop it*; IRM answers *who is doing what, and why*; 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 channel coverage, policy library, and enforcement defaults are actually built around.



Where DLP Sits in the Cyber Stack — DLP, IRM, DSPM, SSE, and AI Security positioned by Channel Coverage × Detection Sophistication

The DLP category sits in the data-flow / enforcement quadrant. IRM shares the people side; DSPM shares the data-classification substrate. SSE bundles DLP modules into the cloud-edge enforcement layer; AI Security entrants are extending DLP into the AI-runtime channel.

What DLP IS. A classification-and-enforcement workflow for data movement. Policies are content-driven (PII, PHI, source code, financial data, IP) and channel-aware (which egress paths are blocked outright, which alert, which are encrypted in-flight, which are watermarked). Enforcement is inline where the buyer has chosen to block (browser uploads, USB writes, SaaS API egress) and asynchronous where they have not (SaaS-API-discovered exposures, retrospective audit). The 2026 DLP product surfaces commonly include: endpoint agent, network/proxy egress inspection, SaaS API connectors, browser extension, email gateway integration, and (newly) AI-runtime hooks for prompt and output inspection [2] [8].

What DLP IS NOT. Not an IRM (the workflow does not centrally orchestrate HR-and-Legal review of a person's risk trajectory; alerts are content-and-channel-centric, not person-centric), not a DSPM alone (DSPM maps data at rest and access paths; DLP enforces on the wire), not an AI Security platform (AI App Sec governs the *runtime* of AI

applications — agents, tool calls, output filtering — while DLP governs *data egress* whether or not it traverses an AI runtime [7]), and not an SSE (SSE bundles DLP as a module of a cloud-edge security platform; a standalone DLP vendor sells the primitive without the full SASE stack).

Three common buyer misconceptions. First: "DLP is a solved problem — we've had it for fifteen years." The Symantec and Forcepoint lineage products that defined the 2010s category were built on regex-and-fingerprint paradigms that, on the public evidence, struggle with semantic data — paraphrased source code, summarized contracts, screenshots of sensitive material. Both incumbents have layered ML and behavioral-analytics modules on top of the heritage classification pipeline [6] [9], but as of 2026 neither has shipped a vendor-flagship AI-runtime-egress capability at the level the AI-native entrants are positioning around [3] [4] [5]. Second: "SSE-bundled DLP from Netskope or Zscaler covers our needs — we don't need a standalone DLP." This is true for cloud-edge channels and increasingly true for browser, but materially less true for endpoint, USB, print, and AI-runtime channels where SSE platforms have shallower coverage than standalone DLP specialists. Third: "AI-runtime DLP is just prompt-inspection — any LLM gateway does it." Prompt inspection is the visible surface; the harder problem is *output* inspection (sensitive content generated by the LLM in response to non-sensitive prompts [10]) and *agent tool-call* inspection (sensitive content moving through an agent's downstream calls [11]). Vendor claims here are not yet stabilized; the 2026 RFP language is forming, with Operant AI currently the only named-outlet-sourced vendor publicly addressing the MCP-protocol-level tool-call inspection problem [11] [12].

2.2 The Terrain

Market sizing — three estimates, NOT averaged. DLP market-size figures diverge by roughly an order of magnitude across named private forecasters depending on whether scope is "DLP software only" or "data loss prevention solutions and services." Fortune Business Insights places the 2026 market at USD 4.22B under a "solutions and services" definition, projecting USD 23.76B by 2034 at 24.10% CAGR [13]. Mordor Intelligence places it at USD 42.87B under what it describes as "strictly DLP software solutions," projecting USD 111.98B by 2031 at 21.17% CAGR; cloud-based held 67.31% of 2025 revenue per the same report [14]. P&S Market Research's USD 4.9B 2025 figure with 21.3% CAGR (2026–2032) [15] sits near the Fortune band. The takeaway is not a precise number — it is that DLP "market size" is a scope-definition question more than a measurement question, and any vendor or buyer citing a single DLP TAM should be asked which definition they are pricing against. Two of three named estimates project low-to-mid 20s CAGR, indicating a market that is structurally growing at AI-and-cloud rates regardless of

which baseline is correct. Gartner discontinued the DLP Magic Quadrant in 2018 and now publishes a Market Guide only [16]; IDC publishes a MarketScape Worldwide DLP Vendor Assessment (2025 edition cited by Forcepoint [17]). Neither publishes a freely accessible TAM number; both shape vendor positioning narrative rather than the dollar-size number.

Buyer trends. Five shifts shape the 2026 DLP buyer. First, *DLP-as-module-of-DSPM-platform consolidation*: Forcepoint positions its 2026 offering as unifying "DSPM, DDR and DLP in an AI-native platform" [18]; Cyberhaven's February 2026 unified platform bundles DSPM + DLP + IRM + AI Security [19]; BigID announced "DSPM-Augmented DLP" on March 24, 2026 [20]; Microsoft Purview ships a productized DLP migration assistant for Symantec and Forcepoint customers [21]. The buying motion has shifted from "buy DLP" to "buy a data-security platform whose DLP module replaces my legacy DLP." Second, *the legacy-DLP rip-and-replace renewal cycle*: a five-vendor consensus (BigID, CrowdStrike, Cyberhaven, GTB, Concentric) in 2026 published material frames Symantec/Forcepoint/McAfee-era DLP as structurally unable to handle cloud-first architectures and AI-driven access [22] [23] [24] [25] [26]. Third, *identity-platform-led DLP*: Palo Alto Networks closed its USD 25B acquisition of CyberArk on February 11, 2026 — the largest transaction in cybersecurity history — with the framing "secure every identity across the enterprise — human, machine, and agentic" [27] [28]. Combined with Prisma Cloud DLP / Prisma SASE / Cortex XSIAM, this reframes DLP as an identity-controlled-access problem. Fourth, *"secure enablement" replaces "block and deny"*: 2026 vendor messaging (Strac, BigID, Nightfall, Concentric, Cyberhaven) converges on language describing a shift from blocking to secure enablement of sanctioned AI usage with redaction at the exfil case [29] [22] [30]. Fifth, *compliance-evidence-generation as a discrete RFP line item*: Strac frames AI DLP as a compliance-evidence-generation tool for SOC 2, HIPAA, GDPR, and EU AI Act Article 10 [29]; Hyperproof's 2026 brief treats DLP as feeding audit-readiness rather than purely preventive control [31].

User trends. The end-user picture has bifurcated. The browser is the new dominant exfil surface — Strac cites that 80% of generative AI data leaks happen in the browser [29]; the user is no longer attaching a file, the user is pasting a prompt. Employees average 66 GenAI applications per organization while only 17% of organizations have technical controls capable of preventing uploads to public AI tools, per IBM's Cost of a Data Breach 2025 cited in 2026 republication [32] [30]. AI-generated content moves both ways across the perimeter: outputs returning to enterprise systems from external models are themselves a classification surface, because the model may have memorized or recombined sensitive material [29] [33]. Vectra's 2026 benchmark places AI-related data-policy violations at 223 per enterprise per month; shadow AI added USD

670,000 to average breach costs in IBM's 2025 data, with 20% of organizations reporting breaches specifically caused by shadow AI [34] [32]. The dominant structural failure mode at the reviewer tier is alert overload, not missed alerts [22] — mirroring the IRM reviewer-fatigue pattern that Microsoft Purview's Triage Agent and Cyberhaven's Linea AI Analyst Agent address in IRM.

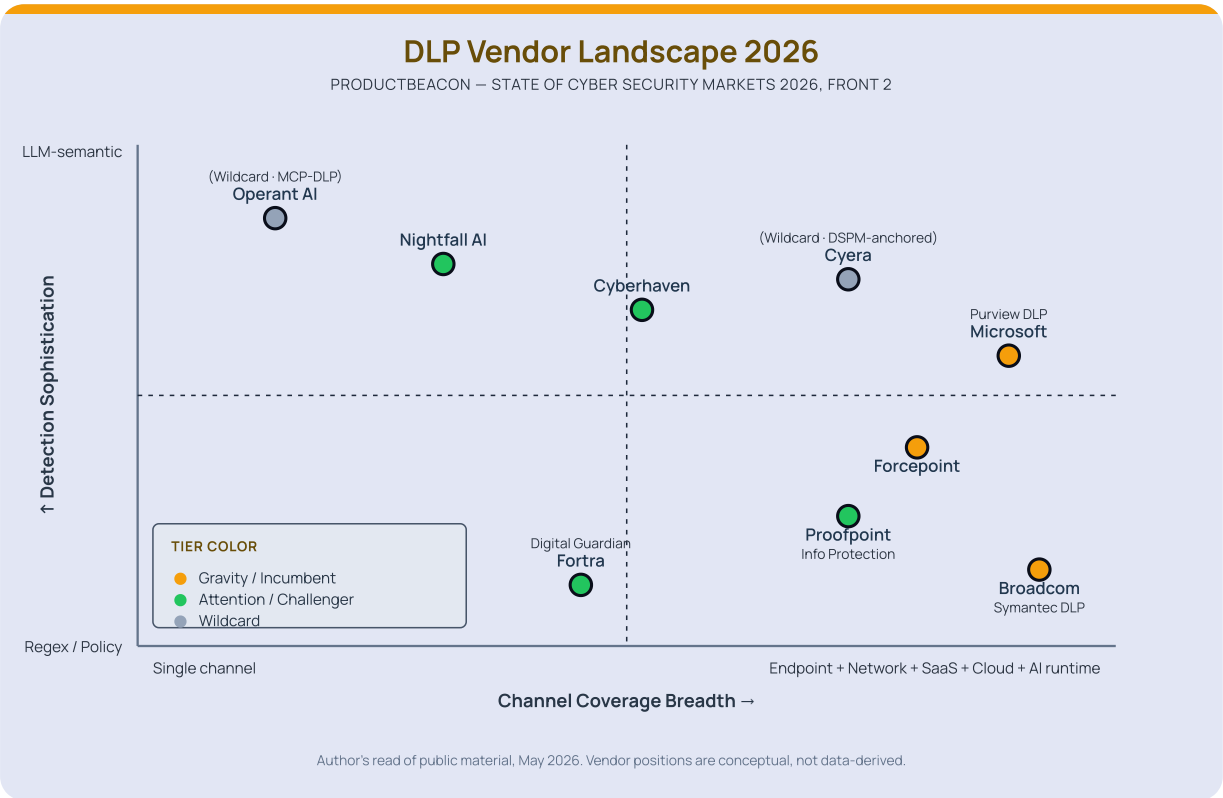
Tech trends. Four shifts. DSPM-augments-DLP convergence is no longer optional — Forcepoint, Cyberhaven, BigID, Microsoft Purview, and Palo Alto Prisma Cloud all bundle DSPM with DLP in 2026 platform pitches [18] [19] [20] [21] [27]. Detection has moved from content-aware to content-and-context-aware via data lineage (where data originated, who touched it, how it moved); Cyberhaven claims 90%+ false-positive reduction via lineage-context versus pattern-match [30], a vendor claim, not independent validation. A four-surface AI DLP architecture has codified in 2026 buyer conversations: Browser DLP (extensions inspecting prompts to ChatGPT/Claude/Gemini), Endpoint DLP (OS-level monitoring of AI coding agents), SaaS DLP (governance of AI connectors), and MCP DLP (auditing Model Context Protocol connections) [29] [35]. MCP itself transitioned "from zero to standard in under twelve months" per Strac's framing [29]; AI agents autonomously connect to databases, source repos, and internal APIs via MCP, with legacy DLP/CASB/proxy controls holding zero visibility into the resulting machine-to-machine traffic [33]. Identity-context has become a primary enforcement input post-Palo Alto/CyberArk close — machine identities outnumber human identities 80-to-1 per the Palo Alto closing release [27], a ratio that argues content-rule DLP cannot scale to machine-identity volume even in principle.

Regulatory trends. Five drivers. EU AI Act Article 10 high-risk-system obligations take effect August 2, 2026 with DLP as a primary control for the data-governance requirements [36] [37]; high-risk categories span biometrics, critical infrastructure, education, employment/HR, essential services, law enforcement, migration, and justice — substantially overlapping regulated-industry DLP buyer profiles. GDPR enforcement has uplifted against AI-data flows, with TechGDPR and IAPP both flagging that GDPR already covers AI personal-data processing and the AI Act adds a second layer rather than a replacement [38] [39]. The US state privacy law mosaic (CCPA/CPRA plus equivalents in CO, CT, UT, VA, plus 2024-2025 additions in TX, FL, OR, MT) now requires jurisdiction-aware policy enforcement in multi-state-operating enterprises [31] [40] [41]. Sectoral rules (HIPAA, PCI-DSS, SOX) have gained AI-specific overlays, creating a budget-bypass channel where AI-DLP gets bought under sectoral renewal even when AI-governance is unbudgeted [31] [30] [42]. And the EU Digital Markets Act Two-Year Review names AI and cloud as priority enforcement areas going into 2026–2027, with

downstream-tenant inheritance effects through Microsoft 365 / Google Workspace / AWS / Azure defaults [43].

2.3 The Contenders

Nine vendors evaluated across three tiers: **3 Gravity** (public or post-$100M private), **4 Attention** (analyst-mentioned, growing into category visibility), and **2 Wildcard** (named-outlet-sourced emerging entrants).



DLP Vendor Landscape 2026 — 9 vendors plotted on Channel Coverage Breadth × Detection Sophistication axes

*Reading the quadrants — **upper-left**: narrow channel + LLM-semantic detection (AI-runtime-first specialists). **Upper-right**: multi-channel + LLM-semantic detection (platform vendors with modern classification). **Lower-left**: narrow channel + regex/policy detection (legacy single-channel tools). **Lower-right**: multi-channel + regex/policy detection (heritage enterprise DLP suites). Tier colors mark Gravity (orange), Attention (green), and Wildcard (grey).*

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

Gravity tier

Microsoft Purview Data Loss Prevention

> *"In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. A DLP policy can help you identify, monitor, and automatically protect sensitive in Enterprise applications & devices and Inline web traffic data." — Microsoft Learn product docs, accessed 2026-05-13* [44]

Purview DLP is the volume leader by distribution reach. The buyer rarely makes a standalone DLP purchase decision — DLP activates as part of a broader Microsoft 365 E5 / E5 Compliance rollout. Stated USP is the breadth of Microsoft 365 signal coverage paired with a layered classification stack (policy templates, exact-data-match, fingerprinting, trainable classifiers, and ML-based adaptive protection scoring user risk into policy) [44] [45]. Microsoft 365 Copilot integration extends classification to prompt-and-output for Microsoft-tenant Copilot specifically [46]. Target buyer is the CISO at a Microsoft-standard enterprise, with purchase routed through the M365 enterprise contract. Pricing signal: bundled inside E5 + Microsoft Purview Suite add-on (user-based) or pay-as-you-go (data-estate-based); no standalone DLP price visible. Architectural classification: SaaS, Microsoft-tenant-bounded, endpoint agent for Windows/macOS/Linux, Edge browser hooks, no inline network proxy. Published-material tier: heavy — Microsoft Learn docs, Mechanics videos, FastTrack rollout playbooks, Gartner Peer Insights footprint, the productized Symantec/Forcepoint migration assistant [21].

Broadcom (Symantec) Data Loss Prevention

Symantec DLP carries the Vontu (2007 Symantec acquisition) → Symantec → Broadcom (2019 acquisition) lineage [47] and is the architectural reference platform that defined the 2010s enterprise-DLP category. Stated USP is multi-channel enterprise DLP across endpoint, network, storage, cloud, and email — the broadest channel-count DLP suite by heritage, with Described Content Matching, Exact Data Matching, Indexed Document Matching, and Vector Machine Learning layered into the classification stack [48]. The combined product naming ("DLP & Data Protection") signals that Broadcom positions Symantec as the DLP layer of a broader Information Protection portfolio, not a standalone hero product; the vendor's hero positioning has migrated up-stack to software-platform framing, with the Vontu lineage preserved in the product name rather than in active hero positioning. Target buyer: Global 2000 enterprise security architect standardized on the Symantec stack, dense in financial services, healthcare,

and government. Pricing: enterprise contract, not public. Architectural classification: hybrid on-prem Enforce server (central policy + incident management) with cloud option; multi-channel detection servers (Endpoint, Network Prevent for Web/Email, Storage, Cloud); regex/EDM/IDM/VML detection stack. Material tier: vendor-controlled thin; named-outlet medium; a decade of Gartner MQ Leader history pre-Broadcom is the strongest external anchor. NASDAQ: AVGO public parent.

Forcepoint Data Loss Prevention

> *"Prevent Data Loss and Adapt to Risk in Real Time. Unify data security for AI, cloud, web, email and endpoint with real-time, intelligent enforcement and sweeping compliance coverage." — Forcepoint DLP product page, accessed 2026-05-13* [49]

Forcepoint is owned by Francisco Partners, with its commercial-side DLP business retained after the January 2024 Everfox carve-out of the federal G2CI business that TPG acquired for USD 2.45B [50] [51]. Stated USP is risk-adaptive DLP — Forcepoint's "Adapt to Risk in Real Time" framing integrates user-behavior risk scoring from Forcepoint Behavioral Analytics into enforcement decisions, structurally differentiated from Symantec's static-policy heritage and Microsoft's bundled-template approach [49] [52]. Lineage: Websense → Raytheon (2015 acquisition of Websense + Stonesoft) → Triton → Forcepoint (2016 rebrand) → Francisco Partners (2021); behavioral-analytics fusion comes from the Raytheon-acquired RedOwl heritage. Target buyer: organizations handling PII/PHI/PCI in hybrid-work environments under multi-jurisdictional regulatory exposure; the page calls out "AI, cloud, web, email and endpoint" as five coverage channels. Pricing: "Request Pricing" CTA only, enterprise contract motion. Architectural classification: hybrid endpoint + on-prem management server + Forcepoint ONE SSE cloud plane, with Risk-Adaptive Protection module cloud-hosted [49] [52]. Material tier: vendor-controlled medium — body copy and analyst-recognition framing fully extractable, post-Everfox-carveout commercial Forcepoint surface healthier than expected.

Attention tier

Cyberhaven

> *"DLP Reimagined. We questioned every assumption and built a DLP solution from the ground up to protect data in a better way." — Cyberhaven DLP product page, accessed 2026-05-13* [53]

Cyberhaven's $100M Series D in April 2025 at $1B post-money valuation [54] crossed the post-$100M-private threshold, but the company's positioning and analyst footprint still sit in the Attention tier rather than Gravity — earnings visibility has not reached public-vendor-grade depth. The dedicated DLP page hero is materially more category-redefining than the corporate homepage ("AI & data security platform unifies DSPM, DLP, Insider Risk, and AI Security"), signaling Cyberhaven's product team positioning the DLP module to win standalone RFPs, not just as a row on a platform-bundle line item. Stated USP is data lineage — the "where did this data come from, who touched it, where is it going" graph — fed into the proprietary "Large Lineage Model" classifier substrate that the vendor markets as enabling "semantic understanding of data, people, and applications…without any rules, definitions, dictionaries, or policies" [53]. Target buyer: AI-era CISO consolidating multiple data-security line items into one platform. Pricing: enterprise subscription, not public. Architectural classification: cloud-analytics plane with multi-source collection (endpoint agent + browser extensions + cloud SaaS apps) — the same architecture as Cyberhaven's IRM module in Front 1, sharing the data-lineage substrate. Material tier: medium — PR Newswire funding cycle, Latka revenue disclosures ($52.4M FY 2026), February 2026 unified platform launch press cycle. Cross-reference: Cyberhaven also appears in IRM Front 1 Attention tier — same vendor, primary DLP primitive evaluated here.

Nightfall AI

> *"Stop data leaks to AI — and everywhere else. Nightfall helps you put data loss prevention on autopilot across AI apps, endpoints, and SaaS." — Nightfall AI homepage, accessed 2026-05-13* [55]

Nightfall is the AI-native cloud DLP positioned from inception around ML-classifier detection rather than regex/fingerprint, with a multi-paradigm AI/ML stack the vendor describes as "100+ AI-based models, LLM based file classifiers and Computer Vision models" [55]. Stated USP is breadth of pre-built classifiers for cloud-native content types (Slack, Microsoft 365, Google Workspace, GitHub, Salesforce, Jira, Confluence, OneDrive, SharePoint, Notion, Zendesk) plus generative-AI tools (ChatGPT, Copilot, Gemini, DeepSeek, Claude, Perplexity), endpoint via lightweight macOS/Windows agent, and browser plugin [55]. Target buyer: "Startups to Fortune 500" — cloud-native

mid-market and enterprise SecOps teams standardizing on SaaS-first DLP, often at SaaS-collaboration-heavy organizations. Pricing: `/pricing` page exists with "6x Average ROI" claim; no tier names on homepage. Architectural classification: cloud-SaaS API-first, deployable in minutes; lightweight endpoint agent + browser plugin for AI-tool coverage. Material tier: medium — TechCrunch, BusinessWire funding announcements, analyst-mentioned in cloud-DLP coverage. **Funding staleness note**: most recent public round is Series B ~$40M in September 2022; the press page shows active 2026 content cadence (2026 AI Agent Risk Report, current webinars) but no Series C announcement at access time [55]. Positioning is current and AI-native; the staleness flag attaches to the war-chest signal, not the messaging substrate.

Fortra (Digital Guardian)

The `digitalguardian.com` domain now 301-redirects to `fortra.com/platform/data-loss-prevention` — the Digital Guardian sub-brand has been absorbed into the Fortra platform [56], parallel to the Code42 → Mimecast Incydr redirect documented in IRM Front 1 Pattern Claim 1. Stated USP is endpoint-led DLP with managed-service deployment option (Digital Guardian Managed Security Program), with deep endpoint agent telemetry across Windows, macOS, and Linux [57]. Lineage: Verdasys (founded 2003, endpoint-DLP pioneer) → Digital Guardian (2014 rebrand) → Code Green Networks network-DLP acquisition (2014) → HelpSystems (2021) → Fortra (2022 portfolio rebrand). Target buyer: regulated-industry CISO with strong endpoint-control requirements; pharma, financial services, and defense-industrial-base customer base historically dense. Pricing: enterprise contract; managed-service tier disclosed in vendor case studies. Architectural classification: endpoint-led, hybrid analytics, content-aware + context-aware + DBRM fingerprinting (structured and unstructured) [57]. Material tier: thin on vendor-controlled; medium on named-outlet (acquisition coverage 2021–2022).

Proofpoint Information Protection

> *"Stop Data Loss — Modernize your data loss prevention program. Prevent data loss from careless, compromised and malicious users." — Proofpoint Enterprise DLP product page, accessed 2026-05-13* [58]

Proofpoint is a Thoma Bravo take-private (August 2021, USD 12.3B transaction value [59]) that reportedly crossed $2B ARR mid-2024 under Thoma Bravo ownership [60]. The Enterprise DLP product is a distinct surface from Insider Threat Management (ITM, which lives in IRM Front 1 [^c4 in IRM chapter]) — same parent company, two distinct product lines. The DLP product family bundles email-DLP heritage with the Dathena AI-

classification engine (2023 acquisition [61]) and Tessian behavioral-AI email DLP (2024 acquisition [62]) — a material architectural reshape across 2023–2024. Stated USP is adaptive, human-centric DLP combining unified-console oversight, Nexus AI classifiers, and cross-channel coverage (email + cloud + endpoint). Target buyer: email-security-led CISO who has standardized on Proofpoint and is rationalizing data-protection line items into the Proofpoint platform. Pricing: not disclosed; per-user bundled into Proofpoint platform pricing. Architectural classification: hybrid — primarily cloud-SaaS for email channel; endpoint agent for endpoint coverage; cloud-hosted management plane. Material tier: vendor-controlled heavy. Pillar surprise: less aggressive than expected — Proofpoint's DLP page does NOT lead with the unified-platform narrative that Cyberhaven, Cyera, and Microsoft Purview lead with. The unified-suite framing surfaces one level up at the Information Protection product family page; on the DLP product page itself Proofpoint sits one structural step behind the 2026 convergence narrative.

Wildcard tier

Cyera

> *"One AI brain. Zero noise. DLP, finally working. Every alert pre-analyzed and ready to act on." — Cyera DLP product page, accessed 2026-05-13* [63]

Cyera closed a USD 400M Series F at $9B post-money in January 2026 — a triple-up from $3B in June 2025 — co-led by Lightspeed, Greenoaks, and Georgian, with Accel, Sapphire, Coatue, Sequoia, Redpoint, and new investor Blackstone participating; three independent named-outlet anchors (Fortune, Calcalist, BusinessWire) plus the company press release [64] [65]. Stated USP per the verbatim DLP product page pillar: AI-native overlay that sits *above* existing DLP tooling rather than replacing it. Architectural reality per `tech-credibility.md`: Cyera is DSPM-primary at founding (2021); the DLP capability ("Omni DLP") is a derivative use of the core AI classification engine, positioned as the unified-decisioning layer consuming signals from upstream enforcement points (legacy Symantec/Forcepoint estates) and presenting prioritized DLP alert workflows [63]. The marketing pillar is DLP-overlay-on-top-of-DSPM; the architectural truth is DSPM-primary with DLP as a layered enforcement module — agentless, cloud-native, no endpoint agent, "<1 day to value" per vendor framing [63]. Cross-segment placement note: Cyera is DSPM-anchored, included in this DLP front because the 2026 vendor narrative explicitly bridges DSPM↔DLP and Cyera's funding

visibility makes it the strongest-sourced emerging-tier vendor in the data-security-platform space. Pricing: `/pricing` link present, no tier names visible, enterprise motion.

Operant AI

> *"Operant AI has launched Operant Endpoint Protector, a new addition to its AI Defense Platform that enables enterprise IT and security teams to discover, detect, and defend against threats across every AI tool, coding agent, and Model Context Protocol (MCP)-connected workflow used by employees, directly at the endpoint where most consequential AI activity takes place." — Help Net Security, republishing Operant launch announcement, 2026-05-04* [66]

Operant AI's homepage leads with "Secure Your AI" and positions broadly as AI-runtime defense, not DLP-specifically; the DLP-relevant positioning is extractable only via named-outlet republication of the May 4, 2026 Endpoint Protector launch (Help Net Security + GlobeNewswire [66] [67]). The product features include multi-dimensional PII/PCI/PHI policies enforced inline within prompts, agent loops, and MCP traffic, with auto-redaction for secrets and keys in motion. Architectural classification per `tech-credibility.md`: multi-component (endpoint agent + MCP Gateway + AI Gatekeeper inline runtime component + cloud management plane). Operant was founded as a Kubernetes/cloud-native runtime-security product before pivoting to AI-runtime egress in 2025–2026; the May 4 endpoint launch added the endpoint-agent leg. The CEO/founder quote names "the largest blind spot in the enterprise security stack" — the endpoint where AI agents actually meet enterprise data. Target buyer: enterprise IT and security teams at organizations where AI agents are actively in production. Pricing: not disclosed. The phrase "MCP DLP" is analyst-coined rather than vendor-claimed at the verbatim level — the chapter describes Operant as participating in a MCP-DLP-shaped category without attributing the literal phrase to Operant's own marketing. Material tier: named-outlet covered, no analyst inclusion yet, no public reference customers in the launch material — the typical early-stage signature.

2.4 Their Plays

Five strategic moves in motion across 2026.

Play 1: The DSPM-Eats-DLP Bundle

- **Observation.** Six of the largest vendors — Microsoft Purview, Forcepoint, Cyberhaven, BigID, Palo Alto Prisma Cloud, and IBM Guardium — 2026-position DLP as a module of a DSPM-anchored data-security platform [68] [69] [70] [71] [72]. Microsoft has shipped a productized Symantec/Forcepoint-to-Purview policy migration assistant that names the legacy DLP leaders as rip-and-replace targets [68].
- **Participants.** Microsoft Purview, Forcepoint, Cyberhaven, BigID, Palo Alto, IBM Guardium, plus the standalone-DLP defenders (Symantec, Fortra Digital Guardian, Proofpoint Enterprise DLP).
- **Conditional outcome.** *If by Q4 2026 at least two of {Microsoft, CrowdStrike, Wiz/Google, Palo Alto Networks, Forcepoint, Cyberhaven, BigID, Cyera} disclose in earnings calls or investor materials enterprise wins framed as "DSPM-platform-replace" against legacy DLP, AND Gartner's next Market Guide for Data Loss Prevention (or Forrester's next Wave) reclassifies DLP as a sub-capability of a broader Data Security Platform category, the platform-bundle motion has reorganized the buying process and standalone-DLP specialists face structural renewal pricing pressure. If H2 2026 produces no such earnings disclosures and the next Gartner/Forrester DLP cycle keeps DLP as a standalone category, the convergence is marketing-tier only and the standalone-DLP specialists hold their lane through 2027.*
- **Evidence.** Forcepoint best-DLP-software comparison [69]; Cyberhaven February 2026 platform launch [70]; BigID DSPM-Augmented DLP announcement [71]; Microsoft migration assistant page [68].

Play 2: Identity-Led DLP Post-Palo Alto/CyberArk

- **Observation.** Palo Alto Networks closed its USD 25B acquisition of CyberArk on February 11, 2026 — the largest cybersecurity acquisition in history — with the closing release framing the combined platform as securing "every identity across the enterprise — human, machine, and agentic" and citing an 80-to-1 machine-vs-human identity ratio [27] [28]. The combined Prisma Cloud DLP + Prisma SASE + CyberArk identity layer reframes DLP downstream of identity rather than upstream of data classification.
- **Participants.** Palo Alto Networks (acquirer), CyberArk (target), with secondary positioning effects on Microsoft Purview (identity-bundled via Entra ID), Cyera

(identity-as-platform-axis), and downstream standalone-DLP specialists.

- **Conditional outcome.** *If by Q4 2026 either (a) Palo Alto Networks earnings disclosures cite the Cortex XSIAM + Prisma Cloud DLP + CyberArk integration as a named contributor to enterprise wins, OR (b) Microsoft Defender / Purview DLP product pages publicly add "Entra ID identity-aware DLP" as a headline capability with named reference customers, OR © Gartner's next Magic Quadrant for SSE or Market Guide for DLP names identity-integration as a baseline requirement rather than a feature, the identity-led pitch has reorganized the DLP enforcement primitive itself. If none of those three signals materialize through 2027 and vendor product pages continue marketing identity-integration as a discrete feature, the Palo Alto/CyberArk thesis is platformization narrative more than enforcement-architecture change.*
- **Evidence.** Palo Alto Networks closing release [27] ; GovCon Wire 25B coverage [28] .

Play 3: MCP-DLP Category Formation

- **Observation.** Model Context Protocol (MCP) transitioned "from zero to standard in under twelve months" per Strac's framing [29] ; legacy DLP, CASB, and proxy controls have zero visibility into machine-to-machine MCP traffic [33] . Operant AI launched Endpoint Protector on May 4, 2026 (Help Net Security + GlobeNewswire) as a category-defining vendor-level entry [66] [67] . Nightfall AI ships an MCP Security product line [33] ; Strac, Integrate.io, and MintMCP have all published 2026 MCP-DLP guides [35] .
- **Participants.** Operant AI (the named-outlet anchor for the category), Nightfall AI (adjacent), plus the broader analyst-coined MCP-DLP category.
- **Conditional outcome.** *Nightfall AI's MCP Security product page predates Operant's launch but reads as a positioning extension of an existing AI-DLP line rather than a dedicated MCP-DLP launch. If by Q4 2026 a second vendor ships an MCP-DLP product with a dedicated launch press cycle (matching Operant's May 2026 cadence — named-outlet coverage, distinct product page, MCP-protocol-level positioning), AND Gartner / IDC / Forrester analyst coverage by H1 2027 names MCP-DLP as a distinct category in a published Market Guide / MarketScape / Wave, the formation is structural and MCP-DLP survives as a discrete category. If by H1 2027 no second vendor launches at that cadence and analyst publications continue treating MCP capability as a sub-feature of AI-DLP, the formation collapses and MCP-DLP becomes a feature of broader AI security DLP.*

- **Evidence.** Help Net Security on Operant launch [66]; Strac MCP-DLP guide [35]; Nightfall MCP Security product page [33].

Play 4: Convergence Platform Race

- **Observation.** Cyberhaven and Cyera both ship unified data-security platforms in 2026 with materially different convergence narratives. Cyberhaven's February 2026 unified launch bundles DSPM + DLP + IRM + AI Security on a data-lineage substrate and markets the DLP module as "DLP Reimagined" — a category-redefining standalone play [53] [70]. Cyera positions its DLP capability as "One AI brain" overlay above existing DLP tooling, anchored in a DSPM-primary architectural foundation [63] [64].
- **Participants.** Cyberhaven (data-lineage-led), Cyera (DSPM-led), plus Microsoft Purview (M365-bundle-led) and Proofpoint Information Protection (email-anchored) as parallel platform motions.
- **Conditional outcome.** *If by Q4 2026 the data-lineage and DSPM-led platform pitches start showing in named-outlet enterprise reference customers as the basis of standalone-DLP-rip-and-replace deals, the convergence platform race is producing real buyer-side displacement. If the same period shows platform pitches winning Marketing voice-share without winning DLP-replacement deals, the convergence is narrative-tier only and standalone-DLP renewal cycles hold.*
- **Evidence.** Cyberhaven DLP page [53]; Cyera DLP product page [63]; Cyberhaven February 2026 launch press [70].

Play 5: Heritage Modernization via Migration Tooling

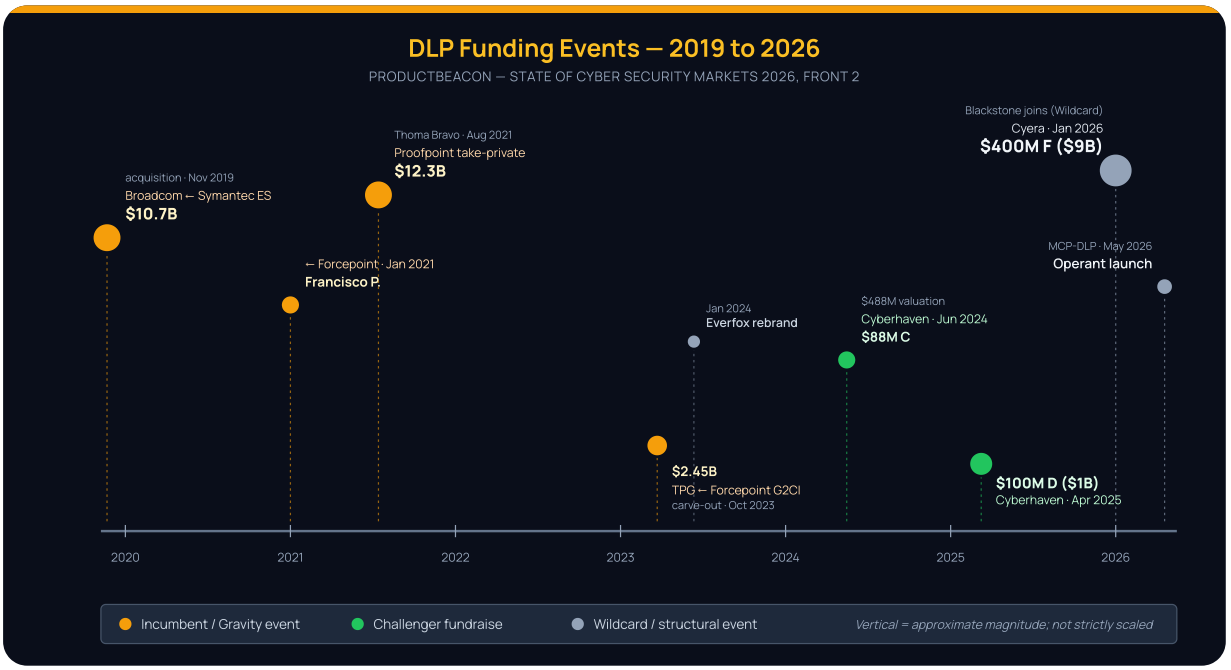
- **Observation.** Microsoft Purview ships a Symantec-and-Forcepoint-to-Purview DLP policy migration assistant as a productized rip-and-replace path [68]. Microsoft does not name Fortra Digital Guardian as a migration target in the tooling, signaling Symantec and Forcepoint specifically as the heritage incumbents being displaced. The five-vendor critic consensus (BigID, CrowdStrike, Cyberhaven, GTB, Concentric) 2026-positions Symantec/Forcepoint/McAfee-era DLP as structurally inadequate for cloud-first and AI-driven access [22] [23] [24] [25] [26].
- **Participants.** Microsoft Purview (migration tool owner), Symantec and Forcepoint (named targets), with secondary effects on Fortra Digital Guardian

(not named in the tooling but in the same 2010s heritage cohort).

- **Conditional outcome.** *If Microsoft's migration assistant generates documented deal flow with named Symantec/Forcepoint reference customers in H2 2026 earnings cycles, the heritage-modernization play is structurally displacing the 2010s-era DLP installed base. If the tooling exists primarily as marketing positioning without flagship-customer migration disclosure, the heritage incumbents retain installed-base inertia through the next renewal cycle.*
- **Evidence.** Microsoft migration assistant docs [68] ; legacy-DLP critique cluster [22] [23] [24] [25] [26] .

2.5 War Chests & Casualties

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



DLP Funding Events — 2019 to 2026, by date, magnitude, and event type

A six-year compression of the DLP money story: Broadcom's $10.7B acquisition of Symantec Enterprise Security in 2019; Thoma Bravo's $12.3B take-private of Proofpoint in 2021; the Cyberhaven Series C-to-D ramp 2024–2025 crossing $1B valuation; TPG's

$2.45B carve-out of Forcepoint G2CI to Everfox in October 2023; and the Cyera Series F at $9B in January 2026 — the largest DLP-adjacent mega-round of the period.

VENDOR	MOST RECENT ROUND	VALUATION (IF PUBLIC)	STRATEGIC INVESTOR	DISTRESS SIGNAL
Microsoft (Purview Data Loss Prevention — module within Microsoft 365 E5 / E5 Compliance) [73]	n/a — bundled within M365 E5 licensing [74]	Public parent (NASDAQ: MSFT); Purview DLP revenue not broken out separately	n/a — incumbent platform	*(empty — no public distress event)*
Broadcom (Symantec Data Loss Prevention — within Broadcom's Enterprise Security Group) [75]	Public — Symantec Enterprise Security acquired by Broadcom in 2019 for ~$10.7B cash; Symantec DLP 25.1 released Oct 1, 2025 [76] [77]	Public (NASDAQ: AVGO); Symantec DLP revenue not separately disclosed	n/a — public parent	*(empty — no public distress event specific to the DLP product line; integration into Enterprise Security Group is positioning fact, not distress)*
Proofpoint (private; DLP via Email DLP + Tessian acquisition + Information Protection suite) [78]	Take-private by Thoma Bravo closed Aug 31, 2021 at $176.00/share cash, ~$12.3B transaction value [79] [80]; ARR crossed $2B mid-2024 under Thoma Bravo ownership [81]	Thoma Bravo (PE sponsor)	*(empty — no public distress event; see IRM front cross-reference for Jan 2024 enterprise-level layoff disclosure)*	
Cyberhaven (data lineage / content-aware DLP) [82]	Series D — $100M led by StepStone Group, with Schroders and Industry Ventures, announced Apr 2, 2025; total funding $250M [83] [84]	StepStone Group (NASDAQ: STEP); prior rounds: Adams Street, Khosla Ventures, Redpoint, Costanoa, Vertex, Wing	$1B post-money valuation (7× in 12 months from $488M Series C in Jun 2024) [85]	*(empty — no public distress event)*
Forcepoint (commercial; private; pure-play data security after Oct 2023 G2CI divestiture) [86]	Acquired by Francisco Partners from Raytheon Technologies in Jan 2021; G2CI government business divested to TPG for $2.45B closing Oct 2, 2023 (rebranded Everfox Jan 2024) [87] [50] [51]	Francisco Partners (PE sponsor)	Private — not disclosed	*(empty — no public distress event; planned CEO succession announced per company PR is positioning fact, not distress)* [88]

VENDOR	MOST RECENT ROUND	VALUATION (IF PUBLIC)	STRATEGIC INVESTOR	DISTRESS SIGNAL
Cyera (Wildcard — DSPM-led platform converging DSPM + DLP + identity) [89]	Series F — $400M co-led by Lightspeed, Greenoaks, Georgian, with Accel, Sapphire, Coatue, Sequoia, Redpoint, and new investor Blackstone, announced Jan 8, 2026; total funding $1.7B+ [64] [65]	Blackstone (NYSE: BX) — new strategic investor in Series F; prior rounds led by Sequoia, Accel, Coatue	$9B post-money valuation (triple-up from $3B in Jun 2025) [90]	*(empty — no public distress event)*

The DLP war chest tilts toward the **scaled incumbents and PE-owned consolidators** more than IRM does. Microsoft Purview DLP, Broadcom-owned Symantec DLP, and Thoma-Bravo-owned Proofpoint together represent the three deepest balance sheets in the segment; none discloses DLP-specific revenue and none carries a same-paragraph distress anchor [73] [76] [81]. The **VC-funded specialist tier** is thinner than IRM's — Cyberhaven is the single $1B-tier pure-play with a 2025-fresh round [84]; Forcepoint's commercial business is a private PE asset reshaped by the $2.45B G2CI divestiture to TPG [50]. **Zero public distress signals** populate the DLP front at access time — a material structural difference from IRM, which carried Varonis's October 2025 re-rating, 5% layoff, and securities class action. The **Wildcard** is Cyera at $9B post-money (Jan 2026 Series F) with Blackstone joining the cap table, materially better-capitalized than the IRM Wildcard cohort [64]. **Watch signal**: Nightfall AI has been funding-silent for over three years (last public round September 2022 Series B [91]) — positioning is current and AI-native, but absent a 2026–2027 round announcement the staleness shifts from messaging to balance-sheet visibility.

> *Not investment advice. See front-matter disclosure.*

2.6 Winning & Losing

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

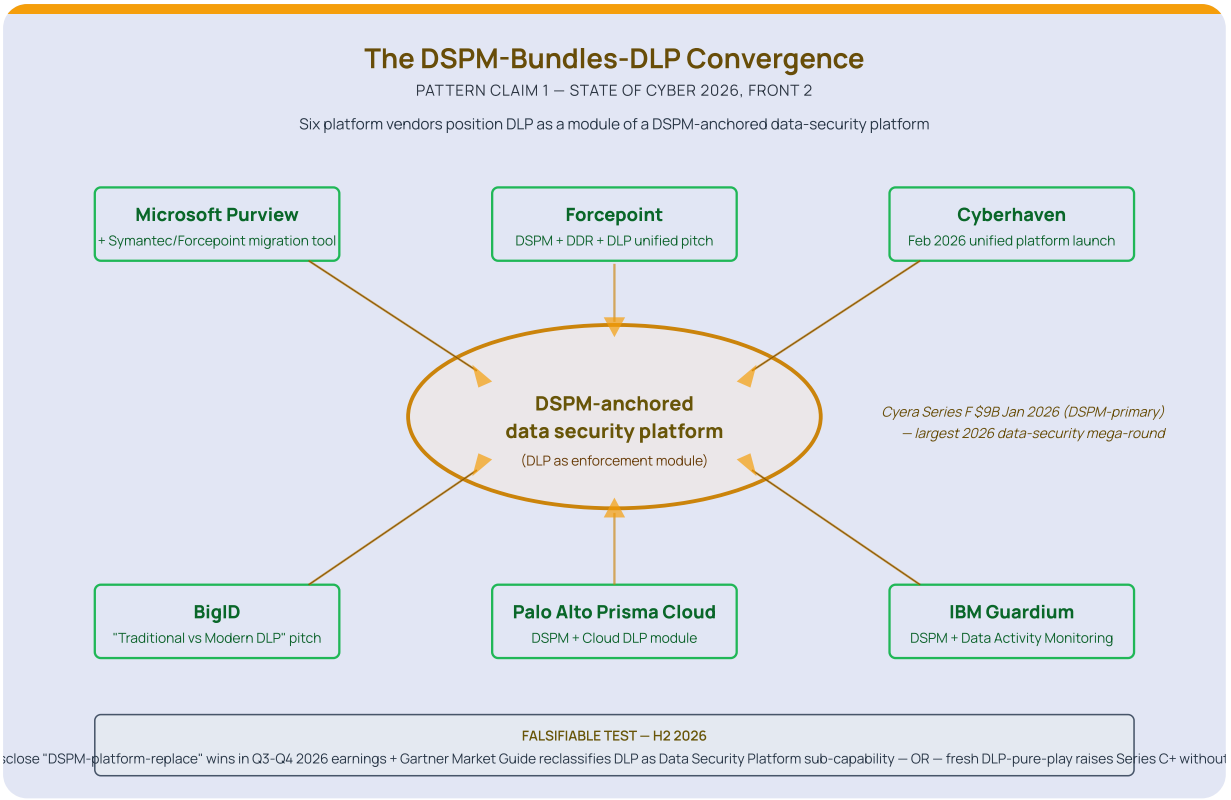
Pattern Claim 1 — The DSPM-Bundles-DLP Convergence

Observation. Six 2026 platform vendors — Microsoft Purview, Forcepoint, Cyberhaven, BigID, Palo Alto Prisma Cloud, and IBM Guardium — explicitly position DLP as a module of a DSPM-anchored data-security platform [92] [93] [94] [95]. Microsoft Purview ships a productized Symantec-and-Forcepoint-to-Purview DLP migration assistant naming the 2010s heritage leaders as rip-and-replace targets [92]. The single largest 2025–2026 data-security mega-round was Cyera's Series F at $9B post-money in January 2026 — a DSPM-primary vendor whose DLP capability is a derivative use of the core AI classification engine [96] [97].

My read. I read this as DSPM absorbing the DLP category narrative the same way Mimecast absorbed the standalone IRM category brand in Front 1's Mimecast Absorption Thesis — but at the *category* level rather than the *vendor* level. The standalone-DLP category brand is being subordinated to a data-security-platform story in which DSPM provides the upstream classification and DLP becomes the downstream enforcement primitive. This is consistent with how 2026 buyer messaging is reorganizing: "buy DLP" has shifted to "buy a data-security platform whose DLP module replaces my legacy DLP."

Conditional prediction. *If the next two data-security mega-rounds (Series E or larger) remain DSPM-led rather than DLP-led, and at least two of {Microsoft, CrowdStrike, Wiz/Google, Palo Alto Networks, Forcepoint, Cyberhaven} disclose in Q3-Q4 2026 earnings calls or investor materials enterprise wins framed as "DSPM-platform-replace" against legacy DLP — AND Gartner's next Market Guide for Data Loss Prevention or Forrester's next Wave reclassifies DLP as a sub-capability of a broader Data Security Platform category — the thesis is structural and standalone-DLP-specialist positioning faces durable renewal pricing pressure. If a fresh independent DLP-pure-play raises a Series C or larger in 2026–2027 without a DSPM-pivot story, AND no major-vendor earnings disclosures cite DSPM-platform-replace deal shapes, the absorption is marketing-tier only and the DLP category brand survives the convergence narrative.*

Sources. [92] [93] [94] [95] [96] [97]



The DSPM-Bundles-DLP Convergence — H2 2026 RFP test: DSPM-platform-with-DLP versus standalone-DLP-line-item

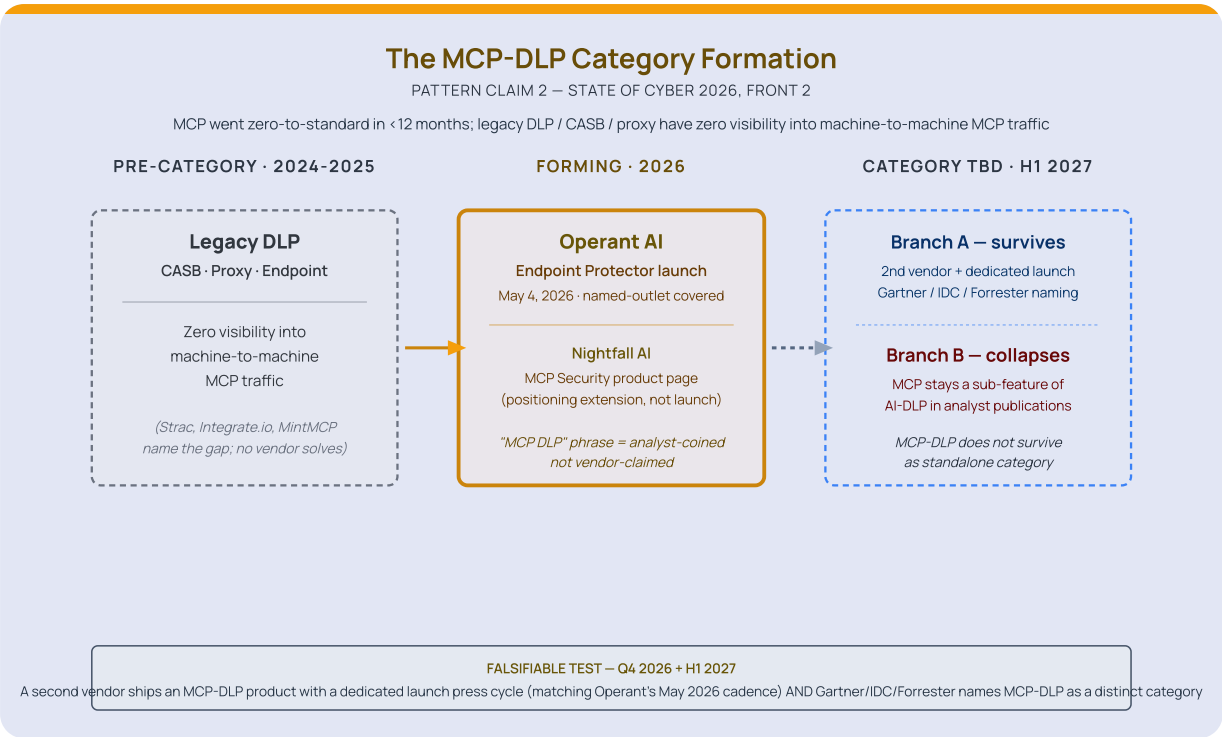
Pattern Claim 2 — The MCP-DLP Category Formation

Observation. Model Context Protocol (MCP) transitioned "from zero to standard in under twelve months" per Strac's framing [98]; AI agents autonomously connect to databases, source repos, file shares, and internal APIs via MCP, with legacy DLP, CASB, and proxy controls holding zero visibility into the resulting machine-to-machine traffic [99]. Operant AI launched Endpoint Protector on May 4, 2026, covered by Help Net Security and GlobeNewswire as a vendor-level entry into the MCP-DLP-shaped capability space [100] [101]. Nightfall AI ships an MCP Security product line as of access date 2026-05-13 [99].

My read. I read this as a genuine category-formation moment with the timing characteristics of a Wildcard window, not a mature category transition. The phrase "MCP DLP" is analyst-coined rather than vendor-claimed — Operant's own homepage leads "Secure Your AI" not "MCP DLP" — which is the structural marker of a category being named by the market before any vendor has earned the right to brand it. Nightfall AI's MCP Security product page predates Operant's launch and is the closest pre-existing vendor surface, but at access date 2026-05-13 it reads as a positioning extension of an existing AI-DLP product line, not a dedicated MCP-DLP product launch with its own press cycle. This claim is framed at category level only — no trajectory inference about Operant itself.

Conditional prediction. *If by Q4 2026 a second vendor ships an MCP-DLP product with a dedicated launch press cycle (matching Operant's May 2026 cadence — named-outlet coverage, distinct product page, MCP-protocol-level positioning) and Gartner / IDC / Forrester analyst coverage names MCP-DLP as a distinct category by H1 2027 in a published Market Guide / MarketScape / Wave, the category is real and MCP-DLP will appear as a discrete entry in analyst publications and vendor product-page taxonomies. If by H1 2027 no second vendor has launched at that cadence and analyst publications continue treating MCP capability as a sub-feature of AI-security-DLP, the formation collapses and MCP-DLP does not survive as a standalone category label.*

Sources. [98] [99] [100] [101]



The MCP-DLP Category Formation — H1 2027 test: second vendor with dedicated launch press cycle + distinct analyst category versus AI-runtime checkbox collapse

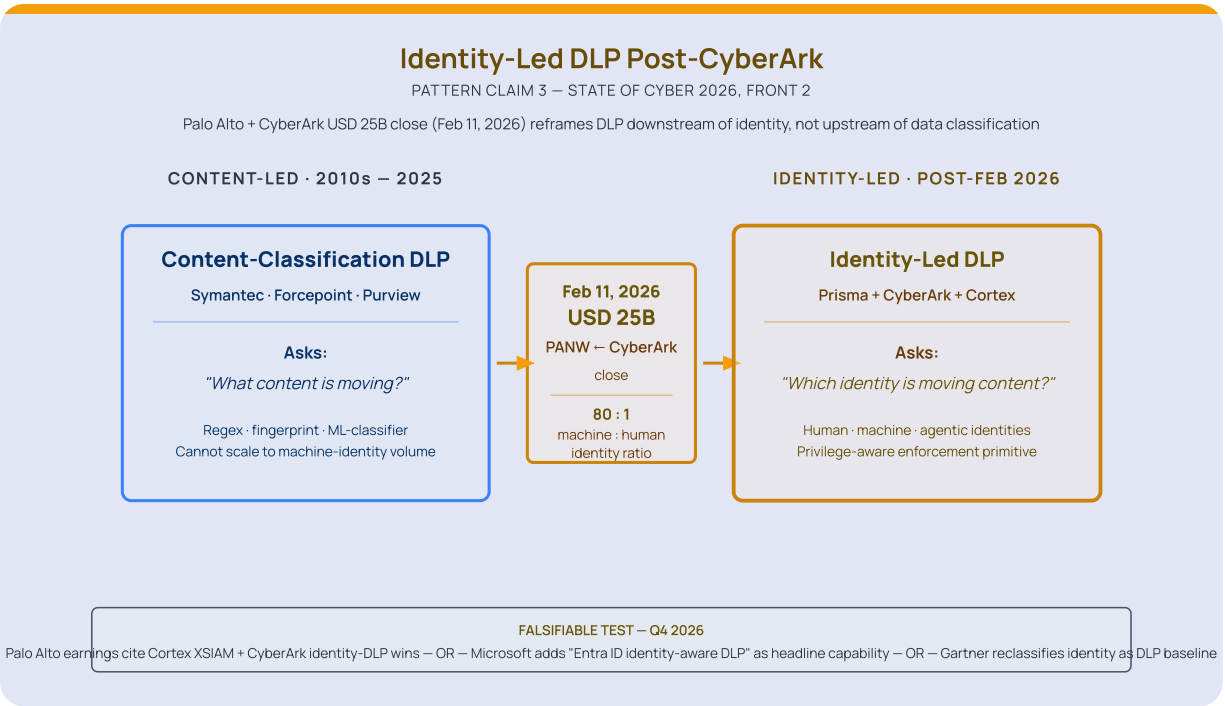
Pattern Claim 3 — Identity-Led DLP Post-CyberArk

Observation. Palo Alto Networks closed its USD 25B acquisition of CyberArk on February 11, 2026 — the largest cybersecurity acquisition in history — framing the combined platform as securing "every identity across the enterprise — human, machine, and agentic" [102] [103]. The closing release cites an 80-to-1 machine-vs-human identity ratio. Combined with Prisma Cloud DLP, Prisma SASE, and Cortex XSIAM, this reframes DLP downstream of identity rather than upstream of data classification.

My read. I read this as a structural reframing of where the DLP enforcement decision is anchored. The historical content-classification-led DLP architecture (Symantec, Forcepoint, Microsoft Purview) asks *what content is moving*; the identity-led pitch asks *which identity is moving content, and is that identity privileged to do so*. The 80-to-1 machine-vs-human ratio is the load-bearing number — content-rule DLP cannot scale to machine-identity volume even in principle, which gives the identity-led pitch a durability that pure platform-bundling does not have. Whether Palo Alto operationalizes this in the enforcement primitive or leaves it as positioning narrative is the open question.

Conditional prediction. *If by Q4 2026 either (a) Palo Alto Networks earnings disclosures cite the Cortex XSIAM + Prisma Cloud DLP + CyberArk integration as a named contributor to enterprise wins; OR (b) Microsoft Defender for Cloud / Purview DLP product pages publicly add "Entra ID identity-aware DLP" as a headline capability with named reference customers; OR © Gartner's next Market Guide for Data Loss Prevention or Magic Quadrant for SSE reclassifies identity-integration as a baseline requirement rather than a feature — the identity-led pitch has reorganized the DLP enforcement primitive and content-classification-led DLP specialists face structural displacement. If none of those three signals materialize through 2027 and vendor product pages continue marketing identity-integration as a discrete feature, the Palo Alto / CyberArk acquisition is platformization narrative rather than enforcement-architecture change.*

Sources. [102] [103]



Identity-Led DLP Post-CyberArk — Q4 2026 RFP test: identity as baseline DLP requirement versus discrete-section parallel

Winners.

- **Microsoft Purview Data Loss Prevention.** Distribution moat via M365 E5 / E5 Compliance bundling is structural. The classification stack layers content-pattern matching, EDM, IDM, trainable classifiers, and ML-based adaptive protection [44] [45], plus the productized Symantec/Forcepoint migration assistant [68] gives Microsoft a productized path to displace heritage incumbents. The Winners label here is opinion-labeled: I read Microsoft's position as winning the *default-choice* slot in Microsoft-standard enterprises, particularly where Copilot integration is in scope, not winning every DLP deal on technical depth.
- **Cyberhaven.** Series D at $1B valuation April 2025 [84], $52.4M revenue (Latka FY 2026), February 2026 unified DSPM + DLP + IRM + AI Security platform launch [70], and a "DLP Reimagined" dedicated DLP page hero [53] that signals product-team commitment to standalone DLP RFPs alongside the unified-platform pitch. Compounded fundraising, revenue, product-platform position, and standalone-DLP positioning simultaneously across a 14-month window.
- **Cyera (Wildcard).** Series F at $9B post-money January 2026 [64] [65] with Blackstone joining the cap table; agentless cloud-native architecture and "One AI brain" DLP-overlay positioning that takes the convergence narrative seriously from a DSPM-primary foundation. The Wildcard placement reflects war-chest depth and named-outlet sourcing rather than a trajectory call.

- **Nightfall AI.** Funding silent for over three years (last public round September 2022 Series B ~$40M [91]). Positioning is current and AI-native, with the multi-paradigm AI/ML stack [55] one of the strongest substrates in the Attention tier. Watch signal: any 2026–2027 round announcement (or its absence). Absent a fresh round, the staleness shifts from messaging to balance-sheet visibility, which downstream RFPs increasingly weight.
- **Forcepoint.** Commercial entity post-Everfox carve-out is structurally a different business than the pre-carve-out Forcepoint, which carried a decade of Gartner MQ Leader history; the G2CI divestiture was a portfolio reshape, not a contraction of the commercial DLP business [50] [51]. Watch signal: H2 2026 product cadence and analyst-recognition presence. The pillar extraction shows the surface healthier than expected [49], holding Gravity tier. The watch is whether the platform-bundle pitch (`forcepoint.com/blog/insights/best-dlp-software` unifies DSPM + DDR + DLP [69]) generates documented buyer-side platform displacement or remains positioning-tier only.
- **Fortra (Digital Guardian).** Portfolio-rebrand pricing visibility is thin; the `digitalguardian.com` 301-redirect to `fortra.com/platform/data-loss-prevention` signals sub-brand absorption [56] parallel to Front 1's Code42 → Mimecast Incydr absorption. Watch signal: hero-pillar refresh on the Fortra platform page, any named-customer reference, or pricing surface changes through H2 2026.
- **Operant AI.** MCP-DLP category-formation trajectory. Watch signal: a second-vendor MCP-DLP entry with a dedicated launch press cycle, analyst inclusion, named reference customers, and any fundraising disclosure beyond the May 2026 launch press cycle.

No DLP 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 DLP business, not a parent-company-wide action. As of May 2026, no DLP Contender meets that bar in the public record reviewed for this chapter. Proofpoint's enterprise-level layoff disclosures cross-reference IRM Front 1's Watch treatment. The Forcepoint CEO succession is company-PR-only and reads as positioning, not distress; the Symantec sub-brand absorption into Broadcom is a positioning fact, not a casualty. Quarterly refreshes will populate this section if DLP-specific signals emerge.

2.7 The Campaign Ahead

Five watchlist items for H2 2026.

1. **MCP-DLP named-vendor #2 emergence.** Signal to monitor: any vendor beyond Operant AI shipping an MCP-protocol-level DLP product with named-outlet republication coverage. Threshold for re-assessment: second vendor entry + analyst recognition (Gartner, IDC, Forrester) naming MCP-DLP as a distinct category → Pattern Claim 2's first branch is realized. Primary source: Help Net Security, GlobeNewswire, SecurityWeek, Gartner Market Guide updates.

1. **DSPM-eats-DLP RFP shift markers.** Signal: enterprise RFP language in named-outlet vendor-win disclosures and Forrester Wave / Gartner Market Guide refresh cycles. Threshold: two or more 2026 Q3–Q4 enterprise DLP wins disclosed as "platform-replace" rather than "DLP-line-item" → Pattern Claim 1's first branch is realized. Primary source: vendor earnings transcripts (where applicable), case studies, named-outlet customer-win coverage.

1. **Cyberhaven DLP-page traction signals.** Signal: standalone "DLP Reimagined" reference customers, analyst recognition for standalone DLP module (separate from the unified-platform claim), revenue trajectory disclosures. Threshold: ARR disclosure crossing $100M with sustained 80%+ growth OR acquisition by a Gravity-tier platform → Gravity-tier reclassification in next refresh. Primary source: Cyberhaven press releases, Latka, PE/strategic-buyer M&A coverage in Reuters and Bloomberg.

1. **Symantec/Broadcom DLP product cadence.** Signal: vendor surface refresh (return-to-extractable-pillar), product release cadence (Symantec DLP 25.1 was October 2025 [77] ; next scheduled release date), and any Gartner Market Guide or IDC MarketScape positioning shift. Threshold for re-assessment: if H2 2026 brings no hero-pillar refresh AND no named product release, a Mimecast-style absorption thesis at the Broadcom level becomes a candidate Pattern Claim at next refresh. Primary source: broadcom.com product page, InvGate ITDB profile, Gartner Market Guide.

1. **Nightfall AI funding event or pivot signal.** Signal: any Series C announcement, valuation update, or M&A disclosure post the September 2022 Series B [91] . Threshold: fresh round at flat-or-up valuation → staleness flag clears, Attention tier confirmed at next refresh; acquisition or down-round (cited from a named

outlet) → Watch escalates to Loser at next refresh. Primary source: Nightfall AI press page, TechCrunch, BusinessWire, SecurityWeek.

Keep reading

Three companion artefacts. Same research, three formats.

NEXT CHAPTER

DSPM

The data-layer that the absorption chain is consolidating around.

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 data loss prevention," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp ↩

2. Broadcom Symantec DLP product page, accessed 2026-05-13.

https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention ↩

3. Cyberhaven Linea product page, accessed 2026-05-13. "Large Lineage Model (LLiM)" verbatim. https://www.cyberhaven.com/product/linea ↩

4. Nightfall AI homepage and product documentation, accessed 2026-05-13. "100+ AI-based models, LLM based file classifiers and Computer Vision models" verbatim. https://www.nightfall.ai/ ↩

5. Cyera homepage, accessed 2026-05-13. "AI-native, enriched classification that learns your business" verbatim. https://www.cyera.com/ ↩

6. Forcepoint Risk-Adaptive Protection product page, accessed 2026-05-13. https://www.forcepoint.com/product/risk-adaptive-protection ↩

7. ProductBeacon, State of Cyber Security Markets 2026 — taxonomy.md §2.1 (IRM ↔ DLP), §2.2 (DLP ↔ DSPM), §2.6 (AI Security ↔ DLP/IRM/DSPM). Internal reference; published with this report. ↩

8. Microsoft Learn, "Microsoft Purview data security and compliance protections for Microsoft 365 Copilot," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/ai-microsoft-purview ↩

9. Proofpoint Press Release, Dathena acquisition June 2023 (vendor URL returned 404 on 2026-05-20 link-audit; cited via Internet Archive snapshot). https://web.archive.org/web/2/*https://www.proofpoint.com/us/newsroom/press-releases/proofpoint-acquires-dathena* ; *Tessian acquisition 2024 (vendor URL returned 404 on 2026-05-20; cited via Internet Archive snapshot).*

https://web.archive.org/web/2/https://www.proofpoint.com/us/newsroom/press-releases/proofpoint-acquires-tessian ↩

10. OWASP Top 10 for Large Language Model Applications 2025, LLM02 "Sensitive Information Disclosure," accessed 2026-05-13. https://owasp.org/www-project-top-10-for-large-language-model-applications/ ↩

11. Anthropic, Model Context Protocol specification, accessed 2026-05-13 (URL re-verified 2026-05-20 — versioned to 2025-11-25). https://modelcontextprotocol.io/specification/2025-11-25 ↩

12. NIST AI 600-1, "Artificial Intelligence Risk Management Framework: Generative AI Profile," July 2024. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf ↩

13. Fortune Business Insights, "Data Loss Prevention Market Size, Share & Forecast, 2034," accessed 2026-05-13. https://www.fortunebusinessinsights.com/data-loss-prevention-market-108686 ↩

14. Mordor Intelligence, "Data Loss Prevention Market Size & Share Analysis (2026–2031)," accessed 2026-05-13. https://www.mordorintelligence.com/industry-reports/data-loss-prevention-market ↩

15. P&S Market Research, "Data Loss Prevention Market Size, and Growth Report, 2032," accessed 2026-05-13. https://www.psmarketresearch.com/market-analysis/data-loss-prevention-market-report ↩

16. Cyberhaven, "What happened to the Gartner Data Loss Prevention Magic Quadrant?" accessed 2026-05-13 (URL re-verified 2026-05-20). https://www.cyberhaven.com/blog/gartner-dlp-magic-quadrant ↩

17. Forcepoint, "IDC MarketScape: Worldwide DLP 2025 Vendor Assessment," accessed 2026-05-13. https://www.forcepoint.com/resources/industry-analyst-reports/idc-marketscape-worldwide-dlp-2025-vendor-assessment ↩

18. Forcepoint, "The Best DLP Software in 2026: Compare Costs and Features," accessed 2026-05-13. https://www.forcepoint.com/blog/insights/best-dlp-software ↩

19. 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 ↩

20. BigID, "DSPM-Augmented DLP" announcement, 2026-03-24, per named-outlet coverage cross-referenced from Strac analysis [^t17]. ↩

21. Microsoft Learn, "Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/dlp-migration-assistant-for-symantec-learn ↩

22. BigID, "Traditional DLP vs Modern DLP: Why Legacy DLP Fails in 2026," accessed 2026-05-13. https://bigid.com/blog/traditional-dlp-vs-modern-dlp/ ↩

23. CrowdStrike, "Five Reasons Why Legacy Data Loss Prevention Tools Fail to Deliver," accessed 2026-05-13. https://www.crowdstrike.com/en-us/blog/five-reasons-legacy-dlp-tools-fail/ ↩

24. Cyberhaven, "Why Legacy DLP Fails: Modern Data Protection Challenges & Solutions," accessed 2026-05-13.

https://www.cyberhaven.com/blog/why-legacy-data-loss-prevention-dlp-fails ↩

25. GTB Technologies, "Replace Your Legacy DLP Solution with DLP that Works," accessed 2026-05-13. https://gttb.com/replace-legacy-dlp-solution-dlp-works/ ↩

26. Concentric AI, "What is Data Loss Prevention (DLP)? 2026 Guide," accessed 2026-05-13. https://concentric.ai/data-loss-prevention-dlp-what-it-means-and-why-traditional-approaches-fall-short/ ↩

27. Palo Alto Networks Press Release, "Palo Alto Networks Completes Acquisition of CyberArk to Secure the AI Era," 2026-02-11. https://www.paloaltonetworks.com/company/press/2026/palo-alto-networks-completes-acquisition-of-cyberark-to-secure-the-ai-era ↩

28. GovCon Wire, "Palo Alto Networks Closes $25B Acquisition of Identity Security Company CyberArk," 2026-02. https://www.govconwire.com/articles/palo-alto-networks-cyberark-25b-acquisition ↩

29. Strac, "AI DLP in 2026: Browser, Endpoint, SaaS & MCP Data Loss Prevention," accessed 2026-05-13. https://www.strac.io/blog/ai-dlp ↩

30. Cyberhaven, "AI Insider Threats: Generative AI Data Leak Risks (2026)," accessed 2026-05-13. https://www.cyberhaven.com/blog/insider-threats-in-the-age-of-ai ↩

31. Hyperproof, "Data Protection Strategies for 2026: Zero Trust and AI Security," accessed 2026-05-13. https://hyperproof.io/resource/data-protection-strategies-for-2026/ ↩

32. IBM Cost of a Data Breach 2025, cited via Aona AI 2026 republication. https://aona.ai/blog/ai-data-loss-prevention/ ↩

33. Nightfall AI, "Model Context Protocol (MCP) Security," accessed 2026-05-13. https://www.nightfall.ai/products/mcp-security ↩

34. Vectra AI, "Shadow AI explained: risks, costs, and enterprise governance," accessed 2026-05-13. https://www.vectra.ai/topics/shadow-ai ↩

35. Strac, "MCP DLP: How to Prevent Data Loss in Model Context Protocol Deployments," accessed 2026-05-13. https://www.strac.io/blog/mcp-dlp ↩

36. Parloa, "AI Privacy Rules: GDPR, EU AI Act, and U.S. Law," accessed 2026-05-13. https://www.parloa.com/blog/AI-privacy-2026/ ↩

37. Secure Privacy, "GDPR Compliance in 2026: The Complete Guide," accessed 2026-05-13. https://secureprivacy.ai/blog/gdpr-compliance-2026 ↩

38. TechGDPR, "Data protection digest 3 Jan 2026," 2026-01-03. https://techgdpr.com/blog/data-protection-digest-03012026-improvements-are-being-made-to-gdpr-enforcement-us-consumer-privacy-and-emerging-shadow-ai/ ↩

39. IAPP, "EU AI Act: Mapping the Interplays with the GDPR," accessed 2026-05-13. https://iapp.org/resources/article/mapping-interplays-gdpr-eu-ai-act ↩

40. Forcepoint, "Global Data Protection Laws in 2026," accessed 2026-05-13.

https://www.forcepoint.com/blog/insights/tracking-global-data-protection-laws-2026 ↩

41. Shadow AI Watch, "AI Data Privacy in 2026: How EU AI Act, GDPR and US State Laws Now Collide," accessed 2026-05-13. https://shadowaiwatch.com/compliance/ai-data-privacy-2026-gdpr-eu-ai-act-us-collision/ ↩

42. Articsledge, "What Is AI DLP? AI-Powered Data Loss Prevention Explained (2026)," accessed 2026-05-13. https://www.articsledge.com/post/artificial-intelligence-data-loss-prevention-ai-dlp ↩

43. ComplianceHub.Wiki, "EU's Digital Markets Act Two-Year Review: AI and Cloud Are Now Priority Enforcement Areas," accessed 2026-05-13. https://compliancehub.wiki/eu-dma-review-ai-cloud-enforcement-2026/ ↩

44. Microsoft Learn, "Learn about data loss prevention," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp ↩

45. Microsoft Learn, "Learn about adaptive protection in Microsoft Purview," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/insider-risk-management-adaptive-protection ↩

46. Microsoft Learn, "Microsoft Purview data security and compliance protections for Microsoft 365 Copilot," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/ai-microsoft-purview ↩

47. Broadcom Press Release, "Broadcom Completes Acquisition of Symantec Enterprise Security Business," 2019-11-04. https://web.archive.org/web/2*/https://investors.broadcom.com/news-releases/news-release-details/broadcom-completes-acquisition-symantec-enterprise-security ↩

48. Broadcom Symantec DLP product page, accessed 2026-05-13; returned title-only at access time; §3.2a invoked. https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention ↩

49. Forcepoint Data Loss Prevention product page, accessed 2026-05-13 (vendor URL returned 404 on 2026-05-20 link-audit; cited via Internet Archive snapshot). https://web.archive.org/web/2*/https://www.forcepoint.com/product/data-loss-prevention-dlp ↩

50. TPG / Forcepoint, "TPG Completes Acquisition of Forcepoint Global Governments and Critical Infrastructure Cybersecurity Business," 2023-10-02. https://www.tpg.com/news-and-insights/tpg-completes-acquisition-of-forcepoint-global-governments-and-critical-infrastructure-cybersecurity-business-from-francisco-partners ↩

51. 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/ ↩

52. Forcepoint Risk-Adaptive Protection product page, accessed 2026-05-13. https://www.forcepoint.com/product/risk-adaptive-protection ↩

53. Cyberhaven DLP product page and Linea product page, accessed 2026-05-13. https://www.cyberhaven.com/product/data-loss-prevention and https://www.cyberhaven.com/product/linea ↩

54. SecurityWeek, "Cyberhaven Banks $100 Million in Series D, Valuation Hits $1 Billion," 2025-04-02. https://www.securityweek.com/cyberhaven-banks-100-million-in-series-d-valuation-hits-1-billion/ ↩

55. Nightfall AI homepage and product documentation, accessed 2026-05-13. https://www.nightfall.ai/ ↩

56. Fortra DLP product surfaces, accessed 2026-05-13; returned HTTP 403 across five paths; §3.2a invoked. https://www.fortra.com/platform/data-loss-prevention ↩

57. Fortra / Digital Guardian Platform Technical Overview white paper, accessed 2026-05-13. https://static.fortra.com/digital-guardian/pdfs/white-paper/dg-platform-technical-overview-wp.pdf ↩

58. Proofpoint Data Loss Prevention product page, accessed 2026-05-13 (URL re-verified 2026-05-20). https://www.proofpoint.com/us/products/data-loss-prevention ↩

59. Proofpoint, "Thoma Bravo Completes Acquisition of Proofpoint," 2021-08-31. https://www.proofpoint.com/us/newsroom/press-releases/thoma-bravo-completes-acquisition-proofpoint ↩

60. Thoma Bravo, "Behind The Deal Podcast Season 4 — Proofpoint," accessed 2026-05-13. https://www.thomabravo.com/behind-the-deal/proofpoint-the-12b-deal-behind-an-ai-driven-cybersecurity-leader ↩

61. Proofpoint Press Release, Dathena acquisition, June 2023 (vendor URL returned 404 on 2026-05-20; cited via Internet Archive snapshot). https://web.archive.org/web/2*/https://www.proofpoint.com/us/newsroom/press-releases/proofpoint-acquires-dathena ↩

62. Proofpoint Press Release, Tessian acquisition, 2024 (vendor URL returned 404 on 2026-05-20; cited via Internet Archive snapshot). https://web.archive.org/web/2*/https://www.proofpoint.com/

us/newsroom/press-releases/proofpoint-acquires-tessian ↩

63. Cyera homepage and DLP product page, accessed 2026-05-13. https://www.cyera.com/platform/data-loss-prevention and https://www.cyera.com/ ↩

64. Fortune, "Exclusive: Cyera CEO Yotam Segev on raising $400 million," 2026-01-08. https://fortune.com/2026/01/08/cyera-cybersecurity-startup-yotam-segev-400-million-series-f-funding-9-billion-valuation-blackstone/ ↩

65. Calcalist Tech, "Cyera hits $9 billion valuation as it announces $400 million Series F." https://www.calcalistech.com/ctechnews/article/s100ccgtvzl ; BusinessWire, "Cyera Raises $400M to Meet Rapidly Growing Demand for AI Security Among Enterprises," 2026-01-08. https://www.businesswire.com/news/home/20260108628439/en/Cyera-Raises-$400M-to-Meet-Rapidly-Growing-Demand-for-AI-Security-Among-Enterprises ↩

66. Help Net Security, "Operant AI Endpoint Protector secures AI agents and MCP tools," 2026-05-04. https://www.helpnetsecurity.com/2026/05/04/operant-ai-endpoint-protector-secures-ai-agents-and-mcp-tools/ ↩

67. GlobeNewswire, "Operant AI Launches Endpoint Protector: Securing Shadow AI, Coding Agents, and MCP Across the Enterprise," 2026-05-04. https://www.globenewswire.com/news-release/2026/05/04/3286769/0/en/operant-ai-launches-endpoint-protector-securing-shadow-ai-coding-agents-and-mcp-across-the-enterprise.html ↩

68. Microsoft Learn, "Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint,"

accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/dlp-migration-assistant-for-symantec-learn ↩

69. Forcepoint, "The Best DLP Software in 2026: Compare Costs and Features," accessed 2026-05-13. https://www.forcepoint.com/blog/insights/best-dlp-software ↩

70. 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 ↩

71. BigID, "Traditional DLP vs Modern DLP: Why Legacy DLP Fails in 2026," accessed 2026-05-13. https://bigid.com/blog/traditional-dlp-vs-modern-dlp/ ↩

72. Forcepoint, "Top 8 DSPM Trends in 2026," accessed 2026-05-13. https://www.forcepoint.com/blog/insights/dspm-trends ↩

73. Microsoft Learn, "Learn about data loss prevention," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp ; Microsoft, "Microsoft Purview Data Security," accessed 2026-05-13 (URL re-verified 2026-05-20 — reorganized to data-security-governance namespace). https://www.microsoft.com/en-us/security/business/data-security-governance/microsoft-purview-data-security ↩

74. Microsoft, "Microsoft Purview Suite — Pricing," accessed 2026-05-13. https://www.microsoft.com/en-us/security/business/purview-suite-pricing ↩

75. Broadcom, "Symantec Data Loss Prevention (DLP) & Data Protection," accessed 2026-05-13.

https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention ↩

76. Broadcom Inc. / Investor Relations, "Broadcom Completes Acquisition of Symantec Enterprise Security Business," 2019-11-04. https://web.archive.org/web/2*/https://investors.broadcom.com/news-releases/news-release-details/broadcom-completes-acquisition-symantec-enterprise-security ↩

77. Broadcom / InvGate ITDB profile, "Symantec Data Loss Prevention — Specs, reviews and EoL info," accessed 2026-05-13 (cites DLP 25.1 release Oct 1, 2025). https://invgate.com/itdb/symantec-data-loss-prevention ↩

78. Proofpoint / Thoma Bravo, "Proofpoint Signs Definitive Agreement to Acquire Tessian," accessed 2026-05-13. https://www.thomabravo.com/press-releases/proofpoint-signs-definitive-agreement-to-acquire-tessian ↩

79. Proofpoint, "Thoma Bravo Completes Acquisition of Proofpoint," 2021-08-31. https://www.proofpoint.com/us/newsroom/press-releases/thoma-bravo-completes-acquisition-proofpoint ↩

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

81. Thoma Bravo, "Behind The Deal Podcast Season 4 — Proofpoint," accessed 2026-05-13. https://www.thomabravo.com/behind-the-deal/proofpoint-the-12b-deal-behind-an-ai-driven-cybersecurity-leader ↩

82. Cyberhaven, "Cyberhaven — AI-Powered Data Security Platform," accessed 2026-05-13.

https://www.cyberhaven.com/ ↩

83. SecurityWeek, "Cyberhaven Banks $100 Million in Series D, Valuation Hits $1 Billion," 2025-04-02. https://www.securityweek.com/cyberhaven-banks-100-million-in-series-d-valuation-hits-1-billion/ ↩

84. PRNewswire, "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 ↩

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

86. Forcepoint, "Newsroom — Forcepoint Named a Leader in the IDC MarketScape for Worldwide Data Loss Prevention 2025," accessed 2026-05-13. https://www.forcepoint.com/newsroom ↩

87. Francisco Partners, "Forcepoint — Investments," accessed 2026-05-13. https://www.franciscopartners.com/investments/forcepoint ↩

88. Forcepoint, "Forcepoint Strengthens Executive Leadership Team to Drive AI-Powered Data Security Innovation," March 2025. https://www.forcepoint.com/newsroom/2025/forcepoint-strengthens-executive-leadership-team-drive-ai-powered-data-security ↩

89. Cyera, "Cyera — Data Security Platform (DSPM + DLP + Identity)," accessed 2026-05-13. https://www.cyera.com/ ↩

90. Calcalist Tech, "Cyber startup Cyera raising hundreds of millions at over $6 billion valuation." https://www.calcalistech.com/ctechnews/article/bka0iddzgl ↩

91. Nightfall AI press page, accessed 2026-05-13 (no fresh round visible since September 2022 Series B). https://www.nightfall.ai/press ↩

92. Microsoft Learn, "Microsoft Purview Data Loss Prevention migration assistant for Symantec and Forcepoint," accessed 2026-05-13. https://learn.microsoft.com/en-us/purview/dlp-migration-assistant-for-symantec-learn ↩

93. Forcepoint, "The Best DLP Software in 2026: Compare Costs and Features," accessed 2026-05-13. https://www.forcepoint.com/blog/insights/best-dlp-software ↩

94. 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 ↩

95. BigID, "Traditional DLP vs Modern DLP: Why Legacy DLP Fails in 2026," accessed 2026-05-13. https://bigid.com/blog/traditional-dlp-vs-modern-dlp/ ↩

96. Fortune, "Exclusive: Cyera CEO Yotam Segev on raising $400 million," 2026-01-08. https://fortune.com/2026/01/08/cyera-cybersecurity-startup-yotam-segev-400-million-series-f-funding-9-billion-valuation-blackstone/ ↩

97. Cyera DLP product page and homepage, accessed 2026-05-13. https://www.cyera.com/platform/data-loss-prevention ↩

98. Strac, "AI DLP in 2026: Browser, Endpoint, SaaS & MCP Data Loss Prevention," accessed 2026-05-13. https://www.strac.io/blog/ai-dlp ↩

99. Nightfall AI, "Model Context Protocol (MCP) Security," accessed 2026-05-13. https://www.nightfall.ai/products/mcp-security ↩

100. Help Net Security, "Operant AI Endpoint Protector secures AI agents and MCP tools," 2026-05-04. https://www.helpnetsecurity.com/2026/05/04/operant-ai-endpoint-protector-secures-ai-agents-and-mcp-tools/ ↩

101. GlobeNewswire, "Operant AI Launches Endpoint Protector," 2026-05-04. https://www.globenewswire.com/news-release/2026/05/04/3286769/0/en/operant-ai-launches-endpoint-protector-securing-shadow-ai-coding-agents-and-mcp-across-the-enterprise.html ↩

102. Palo Alto Networks Press Release, "Palo Alto Networks Completes Acquisition of CyberArk to Secure the AI Era," 2026-02-11. https://www.paloaltonetworks.com/company/press/2026/palo-alto-networks-completes-acquisition-of-cyberark-to-secure-the-ai-era ↩

103. GovCon Wire, "Palo Alto Networks Closes $25B Acquisition of Identity Security Company CyberArk," 2026-02. https://www.govconwire.com/articles/palo-alto-networks-cyberark-25b-acquisition ↩

Disclosures

DISCLOSURE

Disclosure: The author is Head of Product (Fractional) at AXIA, which competes in DLP. 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.