PRODUCTBEACON

# ProductBeacon — State of Cyber Security Markets 2026, Front 6: The Edge Theater

**Yohay Etsion**

Managing Director, ProductBeacon

2026-06-21

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

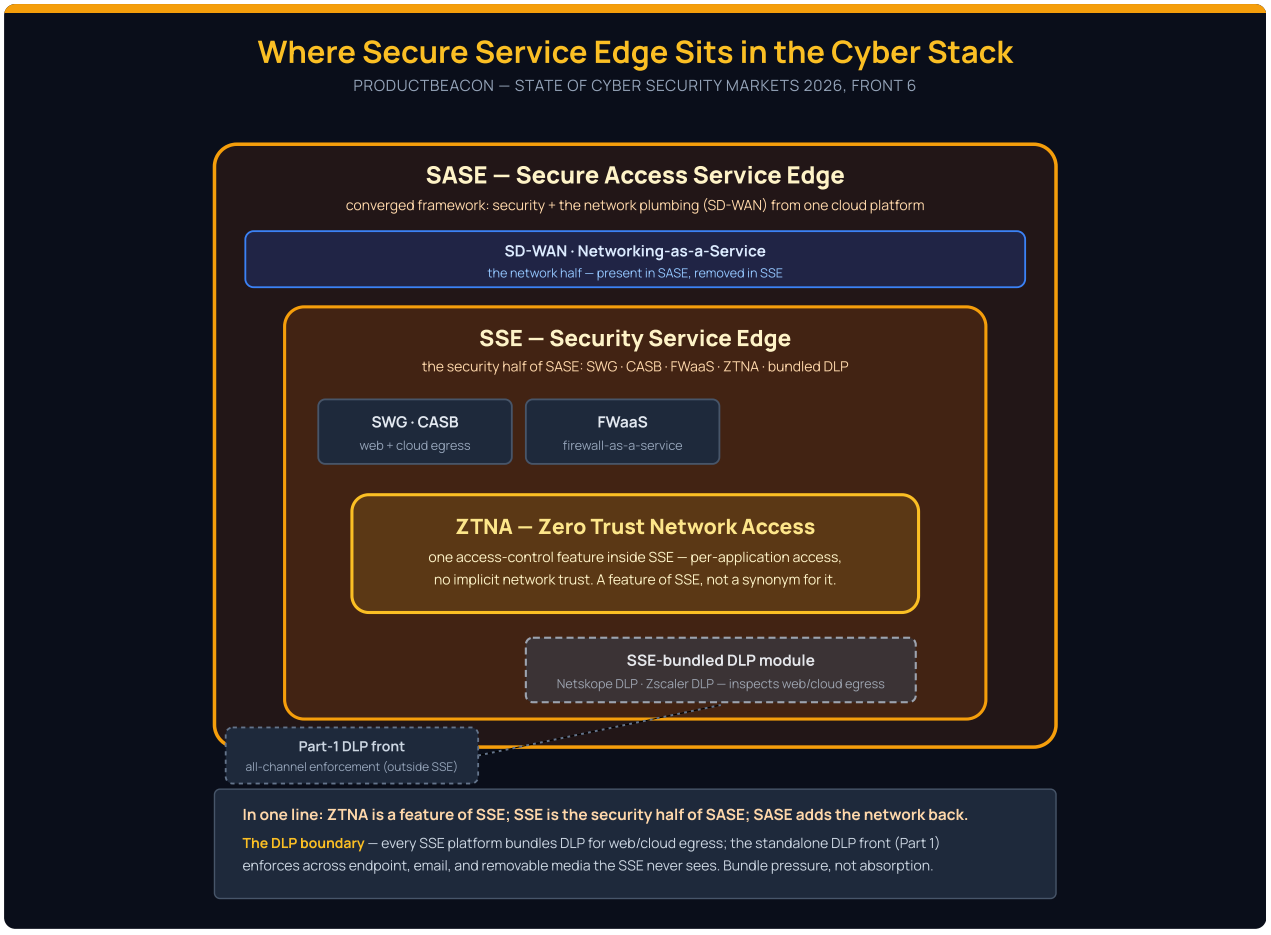
*By Yohay Etsion · Head of Product (Fractional), AXIA · Creator of Product Org OS · Author of Leading the Charge (2023) and Vision to Value (coming 2026)*

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

---

## 6.1 The Playing Ground

The Edge segment is where an organization decides who and what is allowed to reach its applications, and inspects the traffic that flows to and from them, no matter where the user or the workload sits. For two decades that job lived in a hardware perimeter — a firewall at the office, a VPN concentrator for anyone outside it. The cloud and the remote-work shift dissolved that perimeter, and the security stack that replaced it moved to the edge of the network as a cloud-delivered service. Three terms describe that stack, and they are routinely conflated, so it is worth separating them cleanly.




*The wider ring is SASE — networking plus security converged. The inner security half is SSE. ZTNA is one access-control building block inside SSE, not a synonym for it.*

**SASE** (Secure Access Service Edge) is the widest term: the converged framework that delivers software-defined wide-area networking (SD-WAN) *and* security from one cloud platform.[1] **SSE** (Security Service Edge) is the security half of SASE with the networking removed — the bundle of Secure Web Gateway

(SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall-as-a-Service (FWaaS).[2] **ZTNA** (Zero Trust Network Access) is narrower still: the VPN-replacement building block *inside* SSE that grants access to one named application at a time, after verifying identity and device posture, rather than dropping a user onto a flat network.[3] In one line: ZTNA is a feature of SSE; SSE is the security half of SASE; SASE adds the network plumbing back.

What the Edge is *not* is as instructive as what it is. It is not a SOC platform — it enforces and inspects at the egress point, but the detection-investigation-response case workflow belongs to the detection segment, which *consumes* the Edge's anomalous-egress signal rather than the reverse. As the report's cross-front taxonomy frames it, SSE is an *enforcement plane*: it sits in the network-security layer and feeds the SOC, identity, and data-security layers around it.[4]

**The DLP boundary.** This boundary is decisive for the front. Every major SSE platform bundles a data-loss-prevention module — Netskope DLP and Zscaler DLP are the headline examples — because inspecting traffic at the egress is a natural place to stop sensitive data from leaving.[5] That bundled DLP is mentioned here as cross-front presence. The pure-play DLP market is treated as its own front earlier in this report: those are the vendors whose defining capability is data-movement enforcement across every channel, not just the web/cloud egress an SSE sees. The strategic question of whether SSE-bundled DLP displaces the standalone vendors is a winning-and-losing question this front returns to later, not a category line.

Three buyer misconceptions are worth retiring first. One, that **SASE and SSE are the same purchase** — they are not; a buyer who already owns SD-WAN often wants only the SSE half, and vendors price the two separately.[6] Two, that **ZTNA is "just a better VPN."** It replaces the VPN's job, but the architectural difference — per-application access with no implicit network trust — is precisely what narrows the blast radius when a credential is stolen, provided access policies are tightly scoped and continuously re-verified, which a VPN does not. It narrows that radius rather than eliminating it: a stolen, still-valid session token is exactly what the identity-threat-detection layer in the Identity front is there to catch.[7] Three, that **single-vendor SASE is already the default.** Buyer *preference* leans single-vendor, but actual deployments remain stubbornly two-vendor in practice, and the gap between the two is one of the live tensions in this market.[8]

## 6.2 The Terrain

**Market sizing — three lenses, deliberately not averaged.** As with the SOC segment, there is no single Edge number, because analysts size SASE, SSE, and ZTNA as nested-but-distinct categories. Read them side by side. On the widest **SASE** lens, Mordor Intelligence sizes the 2026 market at USD 15.54 billion, growing to USD 39.14 billion by 2031 at a 20.29% CAGR. That definition bundles Network-as-a-Service and Security-as-a-Service across cloud-native, hybrid, and legacy-integrated deployments.[9] MarketsandMarkets frames SASE more aggressively, near USD 19 billion in 2026 on a faster ~29% CAGR.[10] The spread between the two is a definitional artifact of how much SD-WAN and managed networking each firm folds in, which is exactly why averaging them would destroy information. On the narrower **SSE** lens — the security half only — MarketsandMarkets puts the market at USD 6.08 billion in 2024 reaching USD 23.01 billion by 2030 at a 24.8% CAGR, spanning SWG, CASB, ZTNA, and FWaaS, with FWaaS the

fastest-growing component.[11] On the narrowest **ZTNA** lens, 2026 estimates cluster in the low single-digit billions — roughly USD 2.4 billion to USD 4.8 billion. The range depends on whether bundled-into-SSE deployments are counted as ZTNA spend or absorbed into the SSE line, at CAGRs above 20% on every estimate.[12] The honest summary: the narrower the category, the faster the headline growth rate, because spend is migrating *down* the stack from the converged networking story toward the identity-aware access layer.

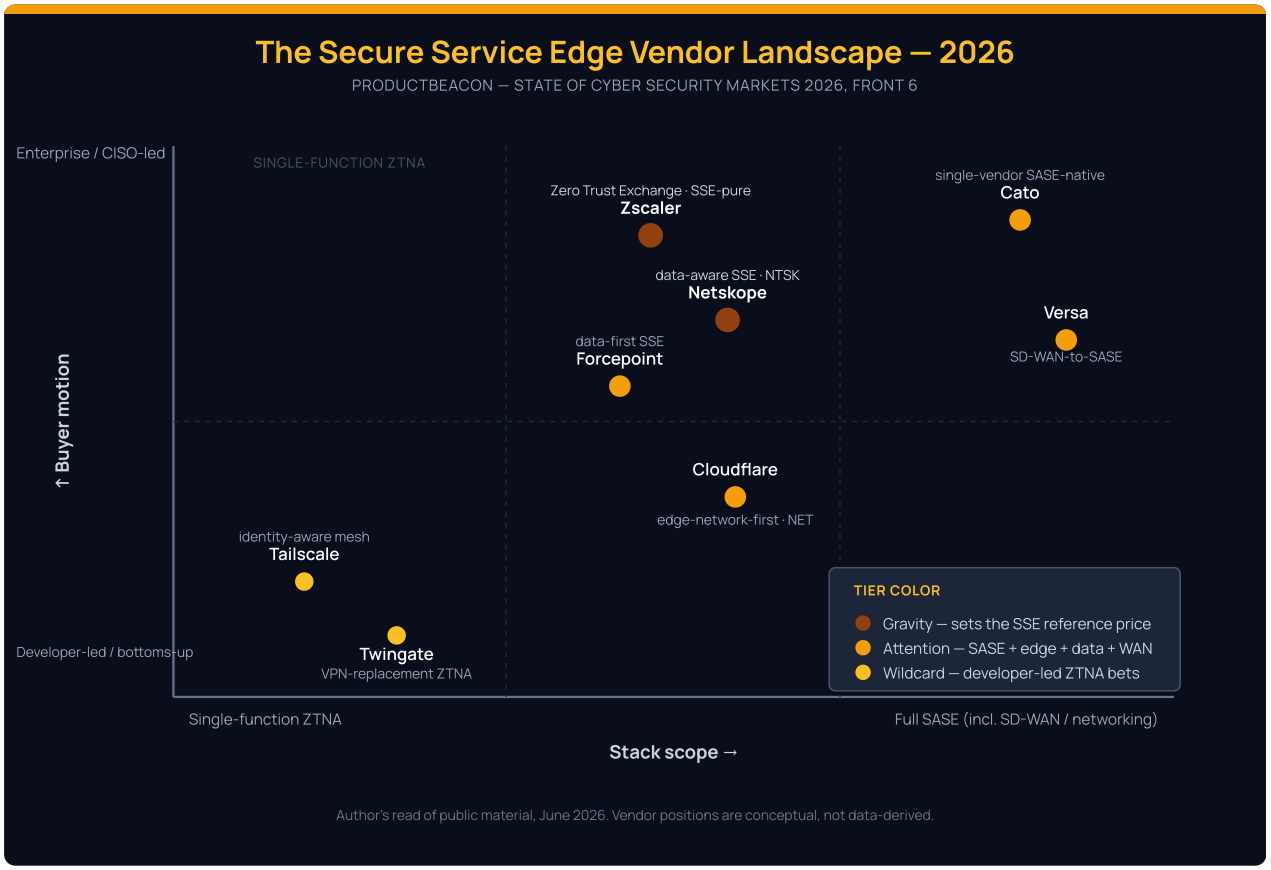
**Buyer trends.** The dominant procurement question is single-vendor versus best-of-breed. Gartner's well-cited (and now-aging) 2022 forecast held that 80% of enterprises would adopt a single-vendor SSE strategy by 2025.[13] The more current signal complicates that. Roughly three in five CISOs prefer single-vendor in principle, but a majority actually deploy two-vendor combinations: SSE from one vendor, SD-WAN from another.[14] I read this preference-versus-practice gap as the defining buyer tension of 2026, and the falsifiable test is public. Watch whether the single-vendor-SASE platform leaders (Fortinet and Cato are named Leaders in Gartner's 2025 SASE Platforms quadrant) grow their disclosed enterprise platform counts faster than best-of-breed SSE pure-plays grow theirs over the next four quarters.[14] A second buyer trend is the VPN-displacement cycle reaching its late innings. The legacy VPN is being retired in favor of ZTNA at scale, with industry surveys reporting a majority of organizations actively replacing VPNs in 2026.[15]

**Technology trends.** Three are reshaping the Edge. The first is **platform consolidation pressure from the SOC platform leaders.** Palo Alto's Prisma Access, Cisco's Umbrella-plus-Hypershield, and Microsoft's Entra Internet Access push SSE as part of a wider bundle, applying the same bundling logic that drives the detection segment. The second, and the one I read as the most consequential for the category's next decade, is the **AI-agent and non-human-identity access problem pushing ZTNA up-market.** Non-human identities — service accounts, API keys, machine tokens, and now autonomous AI agents — already outnumber human identities in many enterprises by ratios reported between 40:1 and over 100:1, and the count is growing fast.[16] ZTNA's per-application, continuously-verified model is the natural control point for an agent that must reach exactly one resource and no more. Zscaler's June 2026 Zenith Live announcement is the clearest production signal. It shipped an AI Broker for agent-to-agent traffic, an Agent Registry, and an AI Access Graph mapping identity-to-data lineage, all repositioning ZTNA from a remote-worker tool toward a machine-identity control plane.[17] My falsifiable prediction, grounded only in observable product-page and earnings signals, runs two ways. If the agentic-access thesis holds, expect the SSE leaders to ship named non-human-identity / agent-access SKUs and report them as growth drivers within the next several quarters. If it is hype, those features stay buried as undifferentiated platform line-items. The third trend is the **architectural divide between network-first and security-first SASE.** Single-stack natives (Cato) and edge-network-first entrants (Cloudflare) are converging on the same category from opposite starting points. That convergence is visible in Netskope's September 2025 Nasdaq IPO (ticker NTSK, ~USD 908 million raised, ~USD 8.6 billion debut valuation), which gave the pure-play SSE thesis its first fully public benchmark.[18]

**Regulatory trends.** The regulatory driver most specific to the Edge is the zero-trust mandate. In the United States, federal civilian agencies operate under binding zero-trust-architecture requirements that explicitly name identity-aware, per-resource access — the ZTNA model — as the target end state. That mandate pulls the public sector onto modern edge platforms on a regulatory timetable rather than a

discretionary one.[19] The broader regulatory tailwind is indirect but real: data-residency and sovereign-cloud obligations in Europe make the *where* of traffic inspection a compliance question, and an SSE platform that can guarantee in-region enforcement points sells directly into that requirement.[20]

## 6.3 The Contenders




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

The edge-security field sorts along two questions. The first is whether the vendor built from the network outward (SD-WAN and SASE heritage) or from the security cloud outward (SSE and ZTNA heritage). The second is whether the buyer is consolidating an entire branch-and-cloud estate onto one platform or buying a single sharp capability — secure private access — and nothing else. The eight vendors below are grouped into three tiers. Gravity holds the two pure-play SSE/ZTNA platforms whose pricing and packaging set the market's reference point. Attention holds the SASE-native challenger, the edge-network incumbent, the repositioning data-security house, and the SD-WAN-to-SASE migrant. Wildcard holds two developer-led ZTNA bets characterized descriptively only. Each card is anchored to a single dated vendor-controlled surface and at least one verbatim messaging pillar lifted from that vendor's live site on 2026-06-16.

## Gravity tier

### Zscaler

> *"Secure Private Access with ZTNA. Extend fast, secure, and reliable private app access for all users from any device or location."* — [Zscaler Private Access, zscaler.com/products-and-solutions/zscaler-private-access, accessed 2026-06-16][21]

Zscaler is the gravity well of this front — the pure-play that built the security-cloud-outward model and proved that a SaaS security edge could displace the appliance stack the rest of the field grew up on. Its stated USP is zero trust delivered as a cloud service: the Zero Trust Exchange brokers every user-to-app connection so that no traffic touches the corporate network and the network itself disappears as an attack surface. Zscaler Private Access carries the ZTNA pillar — "seamless zero trust connectivity for all users, with AI-powered user-to-app segmentation and context-aware policies." Zscaler Internet Access and the broader SSE bundle (secure web gateway, CASB, DLP) cover the outbound side.[22] The target buyer is the large enterprise retiring VPN concentrators and on-premise security appliances; the pricing signal is per-user subscription tiering that rewards bundling the full exchange over single modules. Architecturally Zscaler classifies as SSE-pure and cloud-native, platform-over-best-of-breed — the cleanest articulation of the SSE-first pole. The one fact that complicates the pure-play label is its acquisition of Red Canary, a managed-detection-and-response house, for roughly $651 million completed in August 2025. That move pushes Zscaler across the boundary into the SOC/MDR adjacency mapped in Front 5, blurring the long-standing "we are pure SSE" story.[23] The financials behind the position are the strongest available: in fiscal Q3 2026 (period ended 2026-04-30) Zscaler reported roughly $850 million in revenue, up about 25% year over year, and ARR of roughly $3,525 million, also up about 25%.[24] Published-material tier is the strongest in the front: named-outlet plus SEC-grade (ZS, NASDAQ). My read: Zscaler still sets the SSE reference point the entire field prices against, but the Red Canary move signals it no longer intends to stay inside the SSE box. The pure-play is becoming a platform, and that ambition is the more interesting story than the leadership it already holds.

### Netskope

> *"Netskope: modern security and networking for the cloud and AI era."* — [netskope.com, accessed 2026-06-16][25]

Netskope is the other gravity-tier pure-play, and the detail that an out-of-date read would miss is that it is no longer private. Netskope went public on Nasdaq in September 2025, raising roughly $908 million (47.8 million shares at $19) at a valuation of roughly $8.6 billion.[26] Its stated USP is breadth of the SSE estate delivered from a single cloud. The homepage frames the company as "modern security and networking for the cloud and AI era," and the portfolio spans SSE, CASB, SSPM and DSPM, firewall-as-a-service, and private access — a wider security-data surface than the ZTNA-led pure-plays carry.[25] The target buyer is the enterprise consolidating data-aware web, cloud, and private-access security onto one inline platform. The architecture classifies as SSE-pure and cloud-native, platform-over-best-of-breed,

with data context (the CASB and DSPM heritage) as the differentiating thread. The currency note that matters for any forward read is profitability: in the first half of 2025 Netskope reported ARR of roughly $707 million but remained unprofitable, with a net loss of roughly $170 million for the period. This is a growth-over-margin posture the public markets are now pricing in real time. By its first fiscal quarter as a public company (the quarter ended 2026-04-30) ARR had reached roughly $845 million, up about 29% year over year.[2764] Published-material tier is now the strongest available — newly public reporter (NTSK, NASDAQ) plus named-outlet IPO coverage. My read: Netskope's IPO converts it from a late-stage private peer into a public yardstick alongside Zscaler. Its data-security DNA gives it the most natural overlap with the Part-1 DLP story — the same single platform carries both the SSE and the data-protection module, which is exactly why characterizing it cleanly here matters for cross-front coherence.

## Attention tier

### Cato Networks

> *"World's Leading Single-Vendor SASE Platform. One Platform. Start Anywhere. Grow Everywhere."*
> — [catonetworks.com, accessed 2026-06-16][28]

Cato Networks is the SASE-native challenger — the vendor that built networking and security as one converged cloud service from the ground up rather than stitching SD-WAN and security clouds together after the fact. Its stated USP is single-vendor SASE: the homepage claims the title of "World's Leading Single-Vendor SASE Platform" and frames the architecture as "Cato's SASE platform converges networking, security, and access into a single, global, AI-powered cloud service."[29] The current hero copy has shifted toward an agentic-defense and time-to-patch frame — "From CVE to Protection in Minutes" and "Agentic defense beyond time-to-patch. Cloud-delivered at machine speed" — layering an AI-operations message over the converged-platform foundation.[28] The target buyer is the mid-market-to-enterprise organization that wants one vendor for branch connectivity and security rather than a best-of-breed assembly; the pricing signal is platform subscription rewarding the "start anywhere, grow everywhere" land-and-expand motion. Architecturally Cato is SASE-native and cloud-native, the purest platform-over-best-of-breed play in the set. The capital behind the position is substantial. Cato extended its Series G to roughly $409 million in total at a valuation of more than $4.8 billion (over $1 billion raised across its history). It reports an ARR run-rate of roughly $350 million, up about 43% year over year, with a named place on the 2026 Fortune Cyber 60 for the third year. A public listing that had been discussed has been pushed toward late 2026 or beyond.[30] Published-material tier is named-outlet plus vendor-controlled (funding announcements, analyst lists). My read: Cato has the cleanest architectural story in the Attention tier — genuinely single-vendor, genuinely converged — and the growth rate to back it. That makes it the most credible private threat to the public pure-plays even though its absolute scale still trails them.

### Cloudflare

> *"The agile SASE platform. Connect and protect your workforce, AI agents, and infrastructure."* — [Cloudflare One, cloudflare.com/sase, accessed 2026-06-16][31]

Cloudflare reaches this front from a different starting point than anyone else in the set. It built the largest edge network first and added the security service edge on top, so Cloudflare One is an SSE delivered from infrastructure the company already operated for performance and DDoS protection. Its stated USP is reach and composability. The homepage frames Cloudflare One as "the agile SASE platform" with "SASE architecture unified by design — on a global connectivity cloud," and leans on the network footprint claim that "Cloudflare delivers full SASE from 300+ cities — >3× more than other SASE vendors."[32] The 2026 messaging tilts hard toward AI-era access — "identity-first zero trust access for every employee, contractor, and AI agent," plus first-mover claims on securing connections to MCP servers and on post-quantum encryption across the stack.[31] The target buyer is the organization that already trusts Cloudflare's edge for web performance and wants to extend it into zero-trust access; the pricing signal favors bundling Zero Trust into an existing Cloudflare relationship. Architecturally Cloudflare classifies as edge-network-first and cloud-native, platform-over-best-of-breed by ambition, and it carries a third consecutive year in the Gartner SSE Magic Quadrant. The financials are healthy: Q1 2026 (period ended 2026-03-31) revenue of roughly $639.8 million, up about 34% year over year, with roughly $4.2 billion in cash and roughly $84.1 million in free cash flow. The period also brought an announced workforce reduction of about 20% (1,100-plus roles, framed as an AI-first restructuring) carrying roughly $140-150 million in charges, a note worth registering on organizational health even though it does not change the competitive tier.[33] Published-material tier is named-outlet plus SEC-grade (NET, NYSE). My read: Cloudflare's edge footprint is a structural advantage no pure-play can replicate quickly. But its SSE remains one product line inside a much larger network business — which is both its distribution advantage and the reason its security focus is harder to read than a pure-play's.

### Forcepoint

> *"AI Moves Fast. Your Data Shouldn't Move Uncontrolled. Secure data everywhere from a single platform."* — [forcepoint.com, accessed 2026-06-16][34]

Forcepoint is the data-security incumbent repositioning into the edge — the vendor whose center of gravity is data protection (DLP, classification) and whose SSE story is framed around securing the data flowing through web, cloud, and private access rather than around the network. Its current hero copy makes the data-first frame explicit: "AI Moves Fast. Your Data Shouldn't Move Uncontrolled" and "Secure data everywhere from a single platform," with the AI-era pitch that "AI Is Only as Secure as Your Data" and a claim to "The Most Advanced Data Classification Available."[35] The stated USP is data-aware SSE: protecting sensitive data "across AI tools, cloud apps, web, email, endpoint and network" from one console. The target buyer is the mid-market and regulated-enterprise organization that already knows Forcepoint for DLP and wants its edge security anchored on the same data engine; the pricing signal is platform-and-module subscription aimed at that installed base. Architecturally Forcepoint classifies as

SSE with a data-security center, cloud-delivered, platform-over-best-of-breed within its data-first scope. The ownership structure is the decisive currency fact. Francisco Partners has owned the commercial Forcepoint business since acquiring it from Raytheon in January 2021. The government business (G2CI) was acquired separately by TPG in a deal worth roughly $2.45 billion that closed on 2023-10-02, leaving the commercial SSE entity as a distinct, PE-held company.[36] No new 2026 ownership or capital change surfaced in the bounded scan. Published-material tier is named-outlet (acquisition coverage) plus vendor-controlled; as a private PE-held company there is no public reporter. My read: Forcepoint's data-first framing is its genuine differentiator in a field crowded with network-first and access-first stories. But it competes from a mid-market incumbent position against pure-plays with more capital and faster cloud-native momentum. The repositioning is a defense of its installed base as much as an offensive play.

### Versa Networks

> *"Extend SASE to every part of your network with VersaONE. Universal SASE protects and connects every part of your business — from headquarters to branch, cloud to data center, and every user and device in between."* — [versa-networks.com, accessed 2026-06-16][37]

Versa Networks is the SD-WAN-to-SASE migration story — the vendor that came up through software-defined wide-area networking and has spent the converged-edge era repackaging that heritage as "Universal SASE." Its stated USP is breadth of footprint from a single platform. VersaONE is pitched as "a unified platform with one console, one policy, one data lake, and one OS." It spans networking, security, and access across headquarters, branch, cloud, and data center, with VersaAI layered as "AI FOR SASE" and "SASE FOR AI" across the stack.[38] The target buyer is the distributed enterprise modernizing a large branch-and-WAN estate that wants security folded into the network rather than bought separately. The pricing signal is platform subscription aimed at network-led buyers. Architecturally Versa classifies as SASE with an SD-WAN-network-first heritage, cloud-delivered, platform-over-best-of-breed. The funding picture requires a plain currency note. The latest verifiable round is the $120 million pre-IPO financing led by BlackRock in October 2022 (roughly $632 million raised across its history), and the public listing the company signaled around that round has not been realized in the years since. So this card makes no implication of recent capital or imminent IPO.[39] Published-material tier is named-outlet (the 2022 funding coverage) plus vendor-controlled; as a private company there is no public reporter. My read: Versa has a real footprint among network-led buyers. But the four-year gap since its last verifiable raise and the unrealized IPO are the most honest framing of its current standing — the migration story is sound, the capital and liquidity narrative is the open question.

## Wildcard tier

### Tailscale

> *"The best secure connectivity platform for the AI era. A Zero Trust identity-based connectivity platform that replaces your legacy VPN, SASE, and PAM."* — [tailscale.com, accessed 2026-06-16][40]

Tailscale is the developer-led ZTNA wildcard — the identity-aware mesh that grew bottoms-up inside engineering teams as an easier replacement for the corporate VPN. Descriptively, its surfaces position it as a Zero Trust identity-based connectivity platform that replaces, in its own words, "your legacy VPN, SASE, and PAM" together. The pillars cover "remote access for your global team," "infrastructure access to wherever your resources live, including Kubernetes clusters," and "easy, secure, identity-based access to anything."[41] On its surfaces the described buyer skews toward developers and infrastructure teams adopting it for resource access rather than a security organization rolling out a full edge platform. Architecturally it presents as ZTNA-first and identity-based mesh, cloud-coordinated. On the funding and scope picture, Tailscale raised a $160 million Series C in April 2025 (led by Accel) and acquired Border0, a privileged-access-management vendor, in March 2026. Per its surfaces, that move extends the platform from ZTNA into PAM and frames it as a Zero-Trust platform replacing legacy VPN, SASE, and PAM together.[42] Published-material tier is vendor-controlled plus named-outlet funding and acquisition coverage. As a small, early-stage private vendor, Tailscale is read here descriptively only and sits out of this front's pattern claims — at this stage and scale, the responsible read is positional, not a directional verdict on the company itself.

### Twingate

> *"Security, Performance, Simplicity. Pick Three. Identity-based access for users, services, and AI agents that deploys in minutes, scales to every resource, and finally lets you retire your VPN."* — [twingate.com, accessed 2026-06-16][43]

Twingate is the bottoms-up ZTNA wildcard — the VPN-replacement vendor that, like Tailscale, lands inside teams as an easy zero-trust access layer rather than a top-down platform purchase. Descriptively, its surfaces lead with "Security, Performance, Simplicity. Pick Three" and frame the product as "identity-based access for users, services, and AI agents that deploys in minutes, scales to every resource, and finally lets you retire your VPN," with pillars "Zero Trust with No Boundaries," "Protect Every Click," and "Democratize Privileged Access."[44] The newest descriptive thread on its surfaces is access for AI agents alongside users and services. The described buyer skews toward teams wanting a fast VPN replacement and identity-aware access without a heavy rollout. Architecturally it presents as ZTNA-first and identity-based, cloud-coordinated. On funding, the most recent verifiable round is the $42 million Series B from 2022-04-14 (roughly $67 million raised in total). No newer raise surfaced in the bounded scan, so this card states the 2022 vintage plainly and makes no implication of recent capital.[45] Published-material tier is vendor-controlled plus the 2022 named-outlet funding coverage. As with Tailscale, Twingate is read descriptively only and is held out of this front's pattern claims; at this stage and scale, the responsible read is positional, not a verdict on the vendor.

## 6.4 Their Plays

The edge-security market is not arguing about whether to consolidate the stack. It settled that argument years ago. The argument now is about *who consolidates into whom*, and from which direction the consolidation arrives. It might arrive from a single-vendor SASE fabric built as one system, or from a security-operations platform reaching outward to the edge. It might also arrive from an identity-and-

productivity incumbent folding network access into a bundle the buyer already owns, or from a developer-led access tool graduating up-market into the enterprise. Four plays are in motion in 2026, and each is a different answer to the same question. Below, each is stated as an observation grounded in a public signal, the named participants, and a conditional outcome that resolves against something an outsider can watch happen.

## Play 1: The Single-Vendor-SASE vs Best-of-Breed Consolidation Play

- **Observation.** The two structurally different ways to buy SASE are both putting up real numbers. That keeps the buyer's consolidate-versus-flexibility decision genuinely open. Cato Networks, the single-vendor SASE-native architecture, surpassed $350 million ARR with 43% year-over-year growth in 2025. It raised a Series G that reached roughly $409 million in total — a $359 million round extended in September 2025 — at a valuation above $4.8 billion, explicitly keeping its IPO on ice.[46] On the SSE-pure side, Netskope went public on Nasdaq in September 2025, raising roughly $908 million at about an $8.6 billion valuation on first-half ARR near $707 million.[47] The single-stack vendor sells operational simplicity; the SSE-pure and best-of-breed assemblers sell depth and the freedom to swap any layer. Both theses are funded, and neither has been falsified by the other's growth.
- **Participants.** Cato Networks and Versa Networks on the single-vendor-SASE side (one converged network-plus-security stack); Zscaler and Netskope on the SSE-pure side, around which best-of-breed buyers assemble separate SD-WAN, firewall, and DLP layers.
- **Conditional outcome.** *Watch Cato's trajectory over the next two-to-four quarters. Suppose it converts its Series G war chest into a public filing, or a disclosed enterprise (rather than mid-market) logo mix in named-outlet coverage. We then expect the single-vendor-SASE thesis to validate as an enterprise architecture and not just a mid-market simplification. If instead Cato's IPO stays deferred and its disclosed traction stays concentrated below the enterprise tier while Netskope's and Zscaler's public ARR keeps compounding, the best-of-breed-around-an-SSE-core pattern remains the default enterprise motion. In that case single-vendor SASE stays the mid-market's answer.*
- **Evidence.** Cato Networks, "$359 million at a valuation of more than $4.8 billion," 2025 (prnewswire.com, accessed 2026-06-16); Cato Networks, "Cato Surpasses $350 Million ARR," 2025 (catonetworks.com, accessed 2026-06-16); SecurityWeek, Netskope IPO, September 2025 (securityweek.com, accessed 2026-06-16).

## Play 2: The Incumbent Cross-Front Bundle Pressure Play

- **Observation.** Three platform incumbents are pressuring the SSE pure-plays not on edge-security merit but on bundle economics, by attaching network access to portfolios the buyer already licenses. Microsoft ships Entra Internet Access and Entra Private Access (its Global Secure Access SSE family) alongside Defender for Cloud Apps as its cloud access security broker, positioning SSE as an add-on to an Entra and Microsoft 365 estate.[48] Palo Alto Networks sells Prisma Access as the SSE layer of its broader platform; that portfolio's consolidation muscle is visible in its roughly $25 billion CyberArk acquisition completed in February 2026.[49] Cisco carries Umbrella, Duo, and the Hypershield enforcement fabric into the same accounts where it already sits in the network. The competitive vector is the same in all three cases: the SSE line item competes against a bundle discount a standalone vendor cannot match.[50]

- **Participants.** Microsoft (Entra Internet Access + Entra Private Access + Defender for Cloud Apps), Palo Alto Networks (Prisma Access), and Cisco (Umbrella + Duo + Hypershield) as the bundling incumbents; Zscaler and Netskope as the standalone SSE leaders whose pricing the bundle compresses.[51]
- **Conditional outcome.** *Watch Zscaler's and Netskope's earnings calls over the next two-to-four quarters. If they name competitive displacement by Microsoft-, Palo-Alto-, or Cisco-bundled SSE as a churn or deal-cycle factor, we expect the bundle-pressure thesis to validate as a margin and win-rate force on the standalone SSE leaders. If instead they keep compounding ARR with no bundle-displacement reference in their disclosures, and the incumbents' SSE-specific products stay absent from their own security-segment earnings narratives, the cross-front bundle reads as a checkbox attach. That is an attach rather than a genuine displacement of best-of-breed edge security.*
- **Evidence.** Microsoft Learn, Global Secure Access / Entra Internet Access documentation, 2026 (learn.microsoft.com, accessed 2026-06-16). Palo Alto Networks, Prisma Access product page and CyberArk close coverage, 2026 (paloaltonetworks.com / reuters.com, accessed 2026-06-16). Cisco Umbrella and Hypershield product pages, 2026 (cisco.com, accessed 2026-06-16).

## Play 3: The SSE-to-SOC Boundary Move Play

- **Observation.** Zscaler, a pure-play edge-security vendor, acquired the managed detection and response provider Red Canary for roughly $651 million, completed on 2025-08-01. That pulled an SSE platform across the boundary into detection and response, the core territory of the SOC front.[52] Zscaler's own scale gives it the room to do so: fiscal Q3 2026 revenue near $850 million, up 25% year over year, with ARR around $3,525 million.[53] The strategic claim is that an SSE platform sitting inline on every user-to-app connection already holds the telemetry an MDR service needs, so detection and response is a natural extension of the edge rather than a separate purchase.
- **Participants.** Zscaler (post-Red Canary MDR) as the SSE vendor crossing into the SOC; the detection-and-response incumbents whose managed-service revenue it now contests, analyzed primarily in Front 5; cross-front overlap with the detection-and-response analysis in Front 5.[54]
- **Conditional outcome.** *Watch Zscaler's earnings calls over the next two-to-four quarters. If they cite Red Canary MDR as a named attach or cross-sell driver against its installed SSE base, we expect edge vendors crossing into detection and response to become a recurring acquisition pattern rather than a one-off. If instead Red Canary stays a quiet line item with no cross-sell narrative in Zscaler's disclosures, the deal reads as a capability tuck-in rather than a structural boundary move between the edge and the SOC.*
- **Evidence.** Zscaler, Form 10-Q, period ended 2026-04-30 (sec.gov, accessed 2026-06-16); Red Canary acquisition completed 2025-08-01 (Zscaler press release, accessed 2026-06-16).

## Play 4: The Identity-First ZTNA Up-Market Port Play

- **Observation.** The developer-led, identity-aware ZTNA wedge is testing whether it can graduate from a bottoms-up VPN replacement into an enterprise SSE motion. Tailscale raised a $160 million Series C in April 2025, led by Accel. In March 2026 it acquired Border0 to fold privileged access management into its identity-aware mesh, a feature set that reads as a deliberate move up the enterprise buying committee rather than a developer convenience.[55] Twingate occupies the same

identity-first ZTNA wedge from its Series B base, though without a comparable recent capital event on the public record.[56] The thesis is that an identity-aware overlay that engineers adopt on their own can climb into the enterprise once it carries the access-governance controls a security buyer requires. It would displace legacy VPN from the bottom up while the incumbents push SSE from the top down.

- **Participants.** Tailscale (post-Border0 PAM, identity-aware mesh) and Twingate (ZTNA-first) as the developer-led challengers; the established ZTNA offerings of Zscaler (Private Access) and Netskope (Private Access) as the up-market incumbents they are climbing toward.
- **Conditional outcome.** *Suppose Tailscale's PAM-extended platform shows up in named-outlet enterprise customer references, or a disclosed enterprise-tier funding round, over the next two-to-four quarters. We then expect identity-first ZTNA to validate as a real up-market wedge into the enterprise SSE market. The alternative is that disclosed traction stays concentrated in developer and small-team adoption, with no enterprise-logo or enterprise-round signal from Tailscale or Twingate. In that case the developer-led wedge remains a VPN-replacement layer that the SSE incumbents absorb rather than a path to displacing them.*
- **Evidence.** Tailscale, "Series C," April 2025 (tailscale.com, accessed 2026-06-16); PYMNTS, Tailscale–Border0 acquisition, March 2026 (pymnts.com, accessed 2026-06-16); Tracxn, Twingate funding history (tracxn.com, accessed 2026-06-16).

## 6.5 War Chests & Casualties

The capital picture for the edge front splits along the same line as the contender field: public incumbents financing the move outward from their own balance sheets, and privately held specialists whose last fundraises range from very recent to several years old. The snapshot below mixes both.

| Vendor | Most Recent Round | Valuation (if public) | Strategic Investor | Distress Signal |
|---|---|---|---|---|
| **Netskope** (NASDAQ: NTSK) | Public; IPO Nasdaq Sep 2025, raised ~$908M; ~$1.5B raised pre-IPO[57] | ~$8.6B at IPO | Public-market funded | (empty — no public distress event) |
| **Zscaler** (NASDAQ: ZS) | Public; acquired Red Canary ~$651M; ARR ~$3,525M, fiscal Q3 2026[58] | Public market cap | Public-market funded | (empty — no public distress event) |
| **Cloudflare** (NYSE: NET) | Public; Q1 2026 revenue $639.8M (+34%), ~$4.2B cash[59] | Public market cap | Public-market funded | ~20% workforce reduction (~1,100 roles), $140–150M restructuring charges, AI-first reorg announced May 2026[60] |
| **Cato Networks** (private) | $409M Series G at >$4.8B, 2025; >$1B lifetime; IPO deferred[61] | >$4.8B (private) | Vitruvian, ION Crossover, Lightspeed | (empty — no public distress event) |
| **Tailscale** (private) | $160M Series C, Apr 2025 (Accel); acquired Border0, Mar 2026[62] | Not disclosed | Accel (lead) | (empty — no public distress event) |
| **Versa Networks** (private) | $120M pre-IPO round, 2022 (BlackRock); ~$632M lifetime; IPO unrealized[63] | Not disclosed | BlackRock | (empty — no public distress event) |

The dynamic is asymmetric. The public incumbents extend their footprint off balance-sheet cash, with Zscaler buying its way across the SOC boundary. Cloudflare is the one company carrying a citable recent corporate event, and it is not a failing one. Q1 2026 revenue grew 34% to $639.8 million even as it announced a roughly 20% workforce reduction and $140–150 million in restructuring charges tied to an agentic AI-first operating model. That is a strong-growth company restructuring around AI, not a casualty, and should be read that way. Among the private specialists, capital recency is the tell. Cato's $409 million 2025 Series G and Tailscale's $160 million April 2025 Series C both signal recent strength. Versa, by contrast, last raised in 2022 and has not realized the IPO that round preceded, so its position rests on standalone traction rather than an implied war chest. No other vendor here carries a citable public distress event.

## 6.6 Winning & Losing

The Edge is not contested the way the SOC platform war is contested. There is no single piece of high ground that every vendor is storming at once. Instead, the front is a set of overlapping campaigns fought along the seams between categories. SSE-bundled DLP presses on the standalone data-security vendor below it. Developer-led ZTNA ports up into the enterprise the incumbents thought they owned. And the

single-vendor-SASE native wins the mid-market while the question of whether it can hold the enterprise stays open. The vendors who advance here are the ones who can move *across* a seam: turn a bundled module into a budget displacement, turn a developer tool into a machine-identity control plane, turn operational simplicity into an enterprise reference. The ones who stall are the ones defending a single category line while the spend migrates underneath them.

Three patterns explain the movement, and each is contestable on public evidence. The first is a compression line: the DLP module that ships inside every SSE platform pressing the standalone DLP vendor at the total-cost-of-ownership line. The second is a category in motion: identity-first ZTNA porting up-market, accelerated by the AI-agent access problem, displacing the legacy VPN. The third is an open question with a clock on it: whether single-vendor SASE wins only the mid-market or breaks into the enterprise. Each is a named thesis with an observation, a labeled read, and a falsifiable conditional — not a forecast. Where the evidence points at a Wildcard vendor too small to characterize individually, the claim stays at the category level by design.

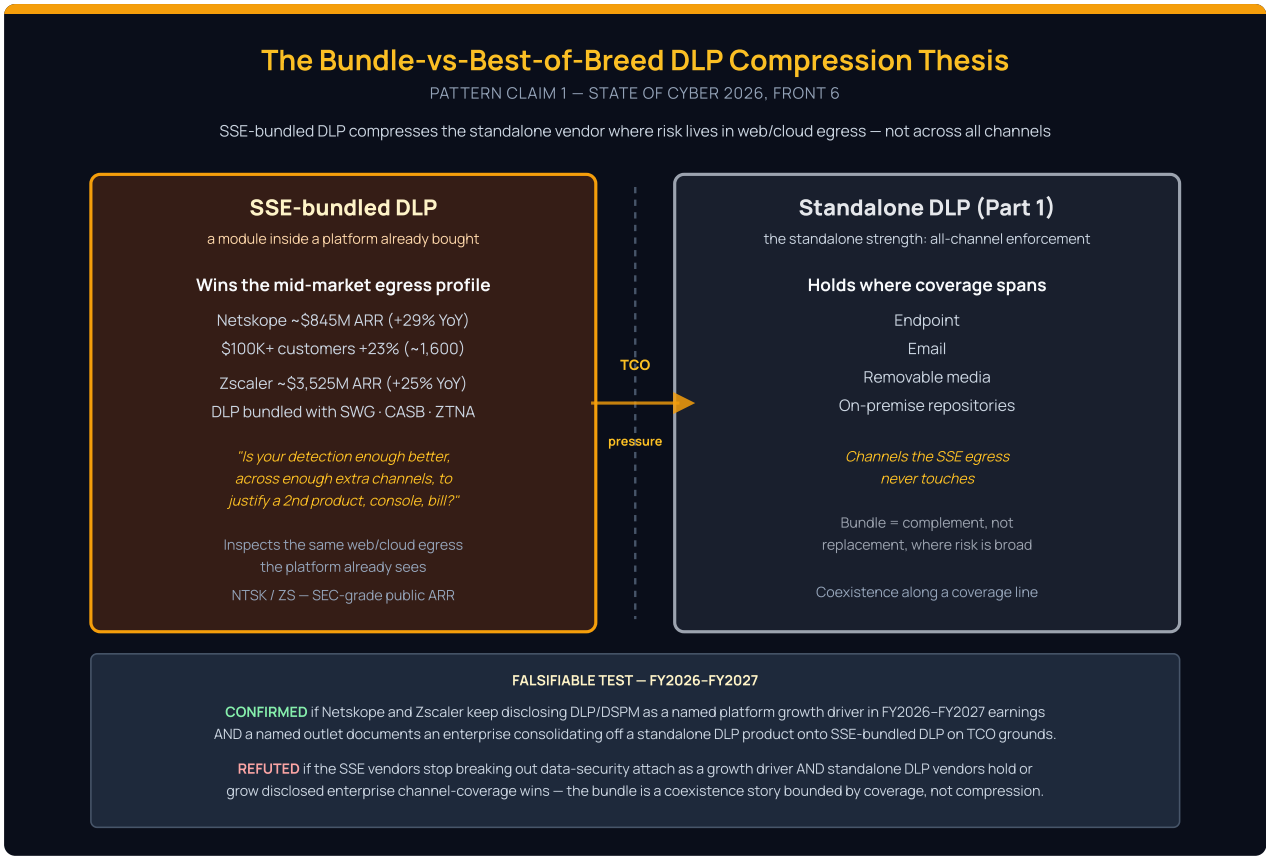
## Pattern Claim 1 — The Bundle-vs-Best-of-Breed DLP Compression Thesis

**Observation.** - Every major SSE platform now ships a data-loss-prevention module as part of the bundle rather than as a separable purchase. - Netskope's platform carries DLP alongside CASB, SSPM, and DSPM. The company reached the public market in September 2025 (Nasdaq: NTSK, ~$8.6B debut valuation, ~$908M raised). - It reported Q1 fiscal 2027 (the quarter ended 2026-04-30) ARR of $845M up 29% year-over-year, with customers paying $100K+ growing 23% to roughly 1,600 [64]. - Zscaler bundles DLP inside its Zero Trust Exchange and reported fiscal Q3 2026 ARR of roughly $3,525M, up about 25% year-over-year [65]. - In both cases the DLP capability reaches the buyer as a line inside a platform the enterprise is already buying for secure web gateway, ZTNA, and CASB — not as a standalone evaluation [66].

**My read.** - I read this as bundled DLP exerting genuine compression on the standalone data-security vendor at the middle of the market, without yet displacing the category at the top. - When a buyer already runs an SSE platform, it can switch on a DLP module that inspects the same web-and-cloud egress the platform already sees. So the competitive question for a standalone DLP vendor stops being "is your detection better" and becomes "is your detection enough better, across enough additional channels, to justify a separate product, a separate console, and a separate bill." - My view is that the SSE bundle wins that argument most often where the buyer's data-movement risk is concentrated in the web and cloud egress the SSE already inspects, which is the mid-market profile. - Where the risk spans endpoint, email, removable media, and on-premise repositories the SSE never touches, the standalone vendor's broader channel coverage still carries the day, and the bundle is a complement rather than a replacement. - This is bundle *pressure* on the standalone DLP front characterized in Part 1, not a verdict that the standalone category is being absorbed. The two coexist along a coverage line.

**Conditional prediction.** - Two conditions confirm the thesis at the middle of the market. First, Netskope and Zscaler continue to disclose DLP/DSPM as a named platform growth driver in FY2026–FY2027 earnings commentary. And second, a named outlet documents an enterprise consolidating off a standalone DLP product onto SSE-bundled DLP specifically on TCO grounds. - If instead the SSE vendors stop breaking out data-security attach as a growth driver, and standalone DLP vendors hold or grow their disclosed enterprise channel-coverage wins through the period, the bundle is a coexistence story bounded by channel coverage, not a compression one.

**Sources.** [64] [65] [66]


The Bundle-vs-Best-of-Breed DLP Compression Thesis
PATTERN CLAIM 1 — STATE OF CYBER 2026, FRONT 6
SSE-bundled DLP compresses the standalone vendor where risk lives in web/cloud egress — not across all channels
SSE-bundled DLP
a module inside a platform already bought
Wins the mid-market egress profile
Netskope ~$845M ARR (+29% YoY)
$100K+ customers +23% (~1,600)
Zscaler ~$3,525M ARR (+25% YoY)
DLP bundled with SWG · CASB · ZTNA
"Is your detection enough better, across enough extra channels, to justify a 2nd product, console, bill?"
Inspects the same web/cloud egress the platform already sees
NTSK / ZS — SEC-grade public ARR
TCO
pressure
Standalone DLP (Part 1)
the standalone strength: all-channel enforcement
Holds where coverage spans
Endpoint
Email
Removable media
On-premise repositories
Channels the SSE egress never touches
Bundle = complement, not replacement, where risk is broad
Coexistence along a coverage line
FALSIFIABLE TEST — FY2026–FY2027
CONFIRMED if Netskope and Zscaler keep disclosing DLP/DSPM as a named platform growth driver in FY2026–FY2027 earnings AND a named outlet documents an enterprise consolidating off a standalone DLP product onto SSE-bundled DLP on TCO grounds.
REFUTED if the SSE vendors stop breaking out data-security attach as a growth driver AND standalone DLP vendors hold or grow disclosed enterprise channel-coverage wins — the bundle is a coexistence story bounded by coverage, not compression.

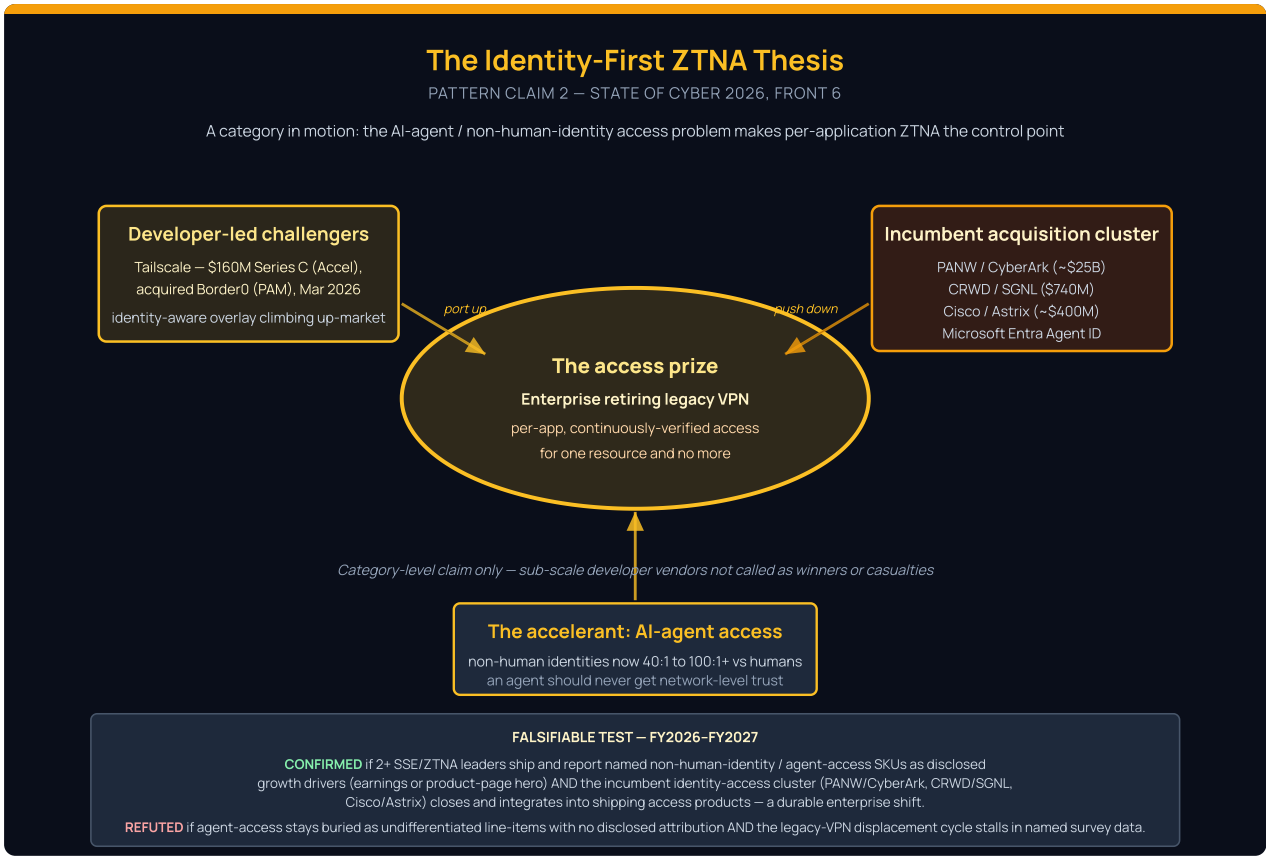
## Pattern Claim 2 — The Identity-First ZTNA Thesis

**Observation.** - The identity-aware access category is heating up on two public signals at once. - Developer-led side first: Tailscale raised a $160M Series C in April 2025, led by Accel. In March 2026 it made its first-ever acquisition, buying privileged-access-management startup Border0[67]. - Bloomberg covered that deal explicitly in the frame of AI agents spilling onto servers and needing per-resource access control. It read the combined entity as a zero-trust access platform reaching beyond VPN replacement into PAM. - Now the incumbent side, where the same access problem is pulling in acquisition capital. Palo Alto Networks completed its roughly $25 billion CyberArk acquisition, closed 2026-02-11. CrowdStrike acquired identity-security firm SGNL for $740M in January 2026. Cisco agreed to acquire non-human-identity vendor Astrix, reported at roughly $400M in May 2026. Microsoft shipped Entra Agent ID to give AI agents first-class identities[68]. - The four moves all aim at the same machine-and-agent access problem. ZTNA's per-application, continuously-verified model is the named enforcement primitive for an agent that must reach exactly one resource and no more[69].

**My read.** - I read this as a category in motion, not a verdict on any single vendor. The signal is the *direction* of capital and product. - Developer-led access tools are climbing up-market through identity-aware policy, and the AI-agent and non-human-identity access problem is the accelerant that makes per-application ZTNA the obvious control point rather than a remote-worker convenience. - My view is that the legacy VPN is the displaced incumbent in this story, because it grants network-level trust an autonomous agent should never receive. The enterprise buyers retiring VPN concentrators are the prize both the developer-led challengers and the platform incumbents are now competing for. - I am deliberately not naming the individual developer-led vendors as winners or casualties. They are early-stage bets whose individual trajectories I cannot responsibly call from public material. - What the public funding rounds and the incumbent acquisition cluster *do* support is the category-level claim: identity-first ZTNA is where the access market is moving, and the AI-agent problem is why it is moving faster.

**Conditional prediction.** - Watch two tests. First, whether two or more SSE/ZTNA platform leaders ship and report named non-human-identity or agent-access SKUs as disclosed growth drivers in FY2026–FY2027 earnings or product-page hero changes. Second, whether the incumbent identity-access acquisition cluster (PANW/CyberArk, CRWD/SGNL, Cisco/Astrix) closes and gets integrated into shipping access products. - If both land, the identity-first ZTNA category motion is confirmed as a durable enterprise shift. - If instead agent-access features stay buried as undifferentiated platform line-items with no disclosed revenue attribution, and the legacy-VPN displacement cycle stalls in named survey data, the thesis is a positioning narrative ahead of budget reality.

**Sources.** [67] [68] [69]


The Identity-First ZTNA Thesis
PATTERN CLAIM 2 — STATE OF CYBER 2026, FRONT 6
A category in motion: the AI-agent / non-human-identity access problem makes per-application ZTNA the control point
Developer-led challengers
Tailscale — $160M Series C (Accel), acquired Border0 (PAM), Mar 2026
identity-aware overlay climbing up-market
port up
push down
Incumbent acquisition cluster
PANW / CyberArk (~$25B)
CRWD / SGNL ($740M)
Cisco / Astrix (~$400M)
Microsoft Entra Agent ID
The access prize
Enterprise retiring legacy VPN
per-app, continuously-verified access
for one resource and no more
Category-level claim only — sub-scale developer vendors not called as winners or casualties
The accelerant: AI-agent access
non-human identities now 40:1 to 100:1+ vs humans
an agent should never get network-level trust
FALSIFIABLE TEST — FY2026–FY2027
CONFIRMED if 2+ SSE/ZTNA leaders ship and report named non-human-identity / agent-access SKUs as disclosed growth drivers (earnings or product-page hero) AND the incumbent identity-access cluster (PANW/CyberArk, CRWD/SGNL, Cisco/Astrix) closes and integrates into shipping access products — a durable enterprise shift.
REFUTED if agent-access stays buried as undifferentiated line-items with no disclosed attribution AND the legacy-VPN displacement cycle stalls in named survey data.

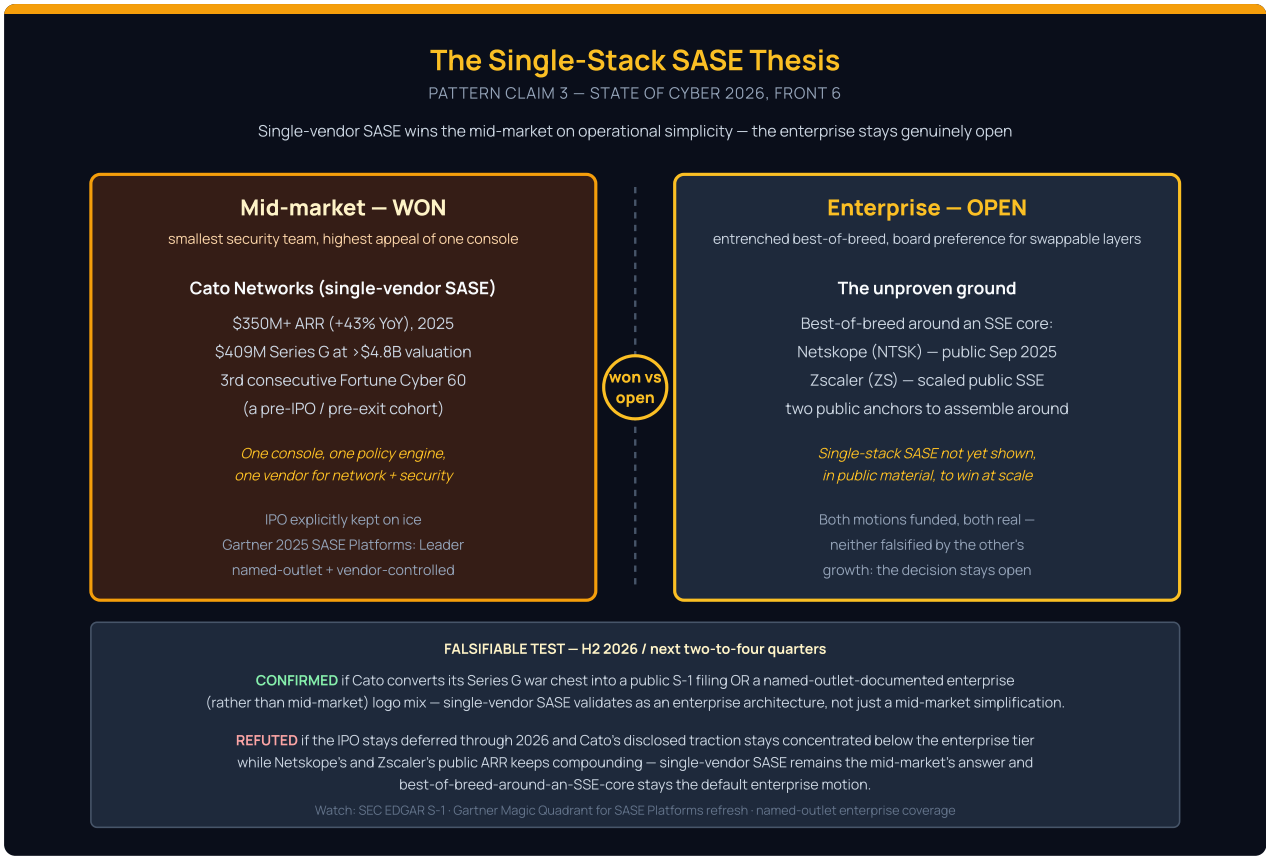
## Pattern Claim 3 — The Single-Stack SASE Thesis

**Observation.** - Cato Networks is the single-vendor-SASE native that built one converged network-plus-security stack from the ground up. - In 2025 it surpassed $350M ARR with 43% year-over-year growth and raised a $409M Series G at a valuation above $4.8 billion, explicitly keeping its IPO on ice [70]. - It was named to the 2026 Fortune Cyber 60 list for a third consecutive year — a venture-backed cohort defined by *not* having had an IPO or exit, which is itself a signal of where Cato sits in its trajectory [71]. - Across the front, the pure-play SSE benchmark moved the other direction. Netskope went public in September 2025, and Zscaler trades as a scaled public SSE platform, giving best-of-breed assemblers two fully public reference points to build around [72].

**My read.** - I read single-vendor SASE as winning the operational-simplicity argument decisively in the mid-market and leaving the enterprise question genuinely open. - Cato's pitch — one console, one policy engine, one vendor for both the network and the security that rides on it — is most valuable precisely where the security team is smallest and the appeal of not integrating four vendors is highest. That is the mid-market profile, and Cato's ARR growth tells me the pitch is converting there. - My view is that the enterprise is the harder, unproven ground. Large organizations with entrenched best-of-breed estates and a board-level preference for swappable layers are the buyers single-stack SASE has not yet been shown, in public material, to win at scale. - The deferred IPO and the Cyber-60 (pre-exit) placement are consistent with a company compounding strongly in its core segment while the enterprise expansion remains the next thing to prove. - The single-stack thesis is not falsified by the best-of-breed vendors' growth, nor they by Cato's. Both motions are funded and both are real, which is exactly what keeps the buyer's consolidate-versus-flexibility decision open.

**Conditional prediction.** - One signal validates the thesis: Cato converts its Series G war chest into a public S-1 filing OR a named-outlet-documented enterprise (rather than mid-market) logo mix over the next two-to-four quarters. That would establish single-vendor SASE as an enterprise architecture and not just a mid-market simplification. - The opposite signal is the IPO staying deferred through 2026, with Cato's disclosed traction concentrated below the enterprise tier while Netskope's and Zscaler's public ARR keeps compounding. In that case single-vendor SASE remains the mid-market's answer, and best-of-breed-around-an-SSE-core stays the default enterprise motion.

**Sources.** [70] [71] [72]




## Winners

**Zscaler** is winning the scaled-platform dimension of the front. Roughly $3,525M in ARR at about 25% year-over-year growth is, in my read, the clearest evidence available that the security-cloud-outward model it pioneered has become the reference point the entire field prices against [65]. My opinion: its moat in 2026 is as much commercial gravity as it is detection efficacy. The buyer who has standardized on the Zero Trust Exchange finds it cheaper to add a module than to evaluate a competitor. And the Red Canary MDR acquisition shows it intends to expand the box rather than defend it [73].

**Netskope** is winning the public-benchmark argument it set out to win. Consider the public record: reaching the Nasdaq in September 2025 at a ~$8.6B debut, and posting Q1 fiscal 2027 (quarter ended 2026-04-30) ARR of $845M up 29% with $100K+ customers up 23%. That, in my view, is the strongest available public evidence that the SSE-pure thesis converts to durable public-market revenue rather than just messaging [64]. It is not winning at Zscaler's scale, but it has given best-of-breed buyers a second fully public SSE anchor to assemble around.

**Cato Networks** is winning the mid-market on operational simplicity. $350M+ ARR at 43% growth and a third consecutive Fortune Cyber 60 placement is, in my read, the clearest public signal that single-vendor SASE has real pull. That pull is strongest where the security team is small and the appeal of one console is highest [70] [71]. The win I am attributing is the mid-market, not the enterprise — that second ground is the open question of Pattern Claim 3.

### Losers / Casualties

This front has few clean casualties, and I will not manufacture one. The honest read is that the Edge is a growth market where the live pressure is compression and displacement *between* growing vendors, not collapse — which is why most of the contested vendors below belong under Watch, not here.

The one dated public restructuring event in the front is **Cloudflare's** May 2026 workforce reduction of approximately 1,100 people (~20% of headcount), announced 2026-05-07 and disclosed in its FY2026 8-K, with charges of $140–150M [74]. I would not label Cloudflare a casualty, and the same source forecloses it. The company framed the action as architecting for an agentic-AI-first operating model — its co-founders stated explicitly that it was not a cost-cutting exercise. That framing sits against a backdrop of a still-growing security and developer-platform business and a Visionary placement in Gartner's 2025 SASE Platforms quadrant [74] [75]. The restructuring is the dated evidence of an AI-first reshaping at a growing company, not a distress signal — and the distinction matters precisely because the headcount number invites the wrong label without the framing the filing supplies.

### Watch

**Cato Networks** is the watch signal I would track most closely on the enterprise-versus-IPO question. The Series G is funded and the ARR is compounding, but the trajectory that resolves Pattern Claim 3 — an S-1 filing or a documented enterprise logo mix — has not yet surfaced in public material [70]. A deferred IPO extending through 2026 without an enterprise-traction disclosure would warrant reassessment at the next refresh; an S-1 would resolve it the other way.

**The developer-led ZTNA category** is the wildcard motion to watch, characterized at the category level only. The public signals — Tailscale's $160M Series C and its Border0 PAM acquisition, and adjacent identity-aware-access positioning elsewhere in the category — point to developer-led access tools porting up-market. But the individual sub-scale vendors are early-stage bets whose individual outcomes I cannot responsibly call from public material [67]. Whether identity-first ZTNA becomes a standalone enterprise wedge or gets absorbed into the platform incumbents' identity-access acquisitions (PANW/CyberArk, CRWD/SGNL, Cisco/Astrix) is the open category question [68].

**Cloudflare** is worth watching post-restructuring on a different axis than its headcount. The question I would track has two sides. Does the agentic-AI-first reorganization translate into shipped, differentiated edge-and-SSE capability that improves its Gartner SASE-quadrant position from Visionary toward the Leaders? Or does the AI-first pivot pull focus from the SSE roadmap while Zscaler and Netskope compound [75]?

## 6.7 The Campaign Ahead

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

1. **SSE-bundled DLP as a disclosed growth driver.** Signal: whether Netskope and Zscaler name DLP/DSPM/data-security attach as a growth driver in their FY2026–FY2027 earnings commentary, plus any named-outlet report of an enterprise consolidating off standalone DLP onto SSE-bundled DLP on TCO grounds. Threshold: a documented standalone-DLP-to-SSE-bundled-DLP consolidation cited specifically on total-cost-of-ownership confirms the compression thesis at the middle of the market; continued attach growth without a documented migration does not. Primary source: Netskope (NASDAQ: NTSK) and Zscaler (NASDAQ: ZS) earnings transcripts and 10-Q filings, plus named-outlet enterprise coverage[76].
2. **Named non-human-identity / agent-access SKUs reported as growth.** Signal: whether two or more SSE/ZTNA leaders ship and disclose named agent-access or non-human-identity SKUs as growth drivers — in earnings commentary or as a product-page hero change — through the period. Threshold: two or more leaders attributing disclosed revenue or pipeline to agent-access SKUs confirms the identity-first ZTNA category motion; agent-access features remaining buried as undifferentiated line-items with no disclosed attribution does not. Primary source: vendor product-page hero snapshots and Zscaler/Netskope earnings transcripts[77].
3. **The incumbent identity-access acquisition cluster closing.** Signal: whether the Palo Alto Networks–CyberArk (~$25B, closed 2026-02-11), CrowdStrike–SGNL ($740M, January 2026), and Cisco–Astrix (reported ~$400M, May 2026) transactions integrate into shipping access products. Threshold: two or more of the three closing and surfacing integrated agent/machine-identity access capability in shipping products confirms the incumbents are competing seriously for the same access ground as the developer-led challengers. Deals stalling or integration not surfacing publicly leaves the category motion unconfirmed on the incumbent side. Primary source: acquirer SEC filings (8-K) and vendor product announcements[78].
4. **Cato's IPO-or-enterprise trajectory.** Signal: whether Cato Networks files a public S-1 or has a named-outlet-documented enterprise (rather than mid-market) logo mix surface, versus a deferral extending through 2026. Threshold: an S-1 filing OR a documented enterprise logo mix validates single-vendor SASE as an enterprise architecture; a continued deferral with traction concentrated below the enterprise tier confirms it as the mid-market's answer. Primary source: SEC EDGAR S-1 filings and named-outlet (Calcalist / SecurityWeek / Bloomberg) enterprise coverage[79].
5. **The Gartner SASE / SSE quadrant refresh.** Signal: the next Gartner Magic Quadrant for SASE Platforms (and the SSE coverage beneath it), and whether Cloudflare moves from Visionary toward Leaders or holds, and whether the pure-play SSE leaders' positions shift relative to the single-vendor-SASE natives. Threshold: a Cloudflare move into the Leaders quadrant confirms the AI-first restructuring translated into category-recognized capability; a held or weakened position signals the pivot pulled focus from the SSE roadmap. Primary source: the published Gartner Magic Quadrant for SASE Platforms / Security Service Edge and vendor announcements citing placement[80].

## References & Footnotes

1. SASE definition — converged cloud-delivered SD-WAN plus security from a single platform. Mordor Intelligence, "Secure Access Service Edge (SASE) Market," accessed 2026-06-16. https://www.mordorintelligence.com/industry-reports/global-secure-access-service-edge-market ↩

2. SSE definition — the security half of SASE comprising SWG, CASB, ZTNA, and FWaaS, with networking removed. MarketsandMarkets, "Security Service Edge (SSE) Market," accessed 2026-06-16. https://www.marketsandmarkets.com/Market-Reports/security-service-edge-market-186280780.html ↩

3. ZTNA definition — per-application access granted after identity and device-posture verification, replacing flat-network VPN access, situated as a component within SSE. MarketsandMarkets, "Security Service Edge (SSE) Market" (ZTNA listed as a core SSE component), accessed 2026-06-16. https://www.marketsandmarkets.com/Market-Reports/security-service-edge-market-186280780.html ↩

4. SSE as an enforcement plane in the network-security layer, feeding SOC / identity / data-security layers (consumed-by-SOC framing). State of Cyber Security Markets 2026, the report's taxonomy §7.1 (Layer 2 — Edge) and §2.5. ↩

5. SSE platforms bundle native DLP modules (Netskope DLP, Zscaler DLP) as cross-front presence; pure-play DLP remains a distinct category. State of Cyber Security Markets 2026, the report's taxonomy §2.5; Netskope IPO portfolio description naming SSE, CASB, and data security posture management. Fintech Global, "Netskope secures $908m as shares debut on Nasdaq," 2025-09-19, accessed 2026-06-16. https://fintech.global/2025/09/19/netskope-secures-908m-as-shares-debut-on-nasdaq/ ↩

6. SASE and SSE are priced and purchased separately; buyers with existing SD-WAN often buy the SSE half only — Gartner's Single-Vendor SASE quadrant evaluates only vendors offering both SSE and SD-WAN, which is why best-of-breed SSE-plus-third-party-SD-WAN combinations sit outside it. Gartner Peer Insights / "Magic Quadrant for SASE Platforms" coverage, accessed 2026-06-16. https://www.gartner.com/reviews/market/single-vendor-sase ↩

7. ZTNA contains blast radius via per-application access with no implicit network trust, unlike a VPN. Portnox, "AI Agent Access Management" (ZTNA per-application enforcement and blast-radius containment), accessed 2026-06-16. https://www.portnox.com/cybersecurity-101/artificial-intelligence/ai-agent-access-management-controlling-what-autonomous-agents-can-do/ ↩

8. Buyer preference leans single-vendor (~61%) while actual deployments remain predominantly two-vendor. Gartner SASE quadrant analysis summary, accessed 2026-06-16. https://sase.cloud/guides/gartner-sase-magic-quadrant-analysis ↩

9. SASE market USD 15.54B (2026) → USD 39.14B (2031) at 20.29% CAGR, on a NaaS-plus-SECaaS definition across cloud-native, hybrid, and legacy-integrated deployments. Mordor Intelligence, "Secure Access Service Edge (SASE) Market," accessed 2026-06-16. https://www.mordorintelligence.com/industry-reports/global-secure-access-service-edge-market ↩

10. SASE market ~USD 19.19B (2026) → USD 68.06B (2032) at ~28.8% CAGR on MarketsandMarkets' broader networking-inclusive definition; the spread versus Mordor reflects how much SD-WAN / managed networking each firm includes. MarketsandMarkets, "Secure Access Service Edge (SASE) Market Report 2026-2032," accessed 2026-06-16. https://www.marketsandmarkets.com/Market-Reports/secure-access-service-edge-market-220384224.html ↩

11. SSE market (security half only) USD 6.08B (2024) → USD 23.01B (2030) at 24.8% CAGR, spanning SWG/CASB/ZTNA/FWaaS, with FWaaS the fastest-growing component. MarketsandMarkets, "Security Service Edge (SSE) Market," accessed 2026-06-16. https://www.marketsandmarkets.com/Market-Reports/security-service-edge-market-186280780.html ↩

12. ZTNA 2026 estimates range ~USD 2.4B–4.8B depending on whether bundled-into-SSE deployments are counted as ZTNA or absorbed into the SSE line, all at CAGRs above 20%. Grand View Research, "Zero Trust Network Access Market," accessed 2026-06-16, https://www.grandviewresearch.com/industry-analysis/zero-trust-

network-access-market-report ; market.us, “Zero Trust Network Access Market” (CAGR ~27%), accessed 2026-06-16, https://market.us/report/zero-trust-network-access-market/ ↩

13. Gartner forecast (Predicts 2022, now aging) that 80% of enterprises would adopt a single-vendor SSE strategy by 2025 — dated 2022 vintage, cited here as the consolidation-thesis anchor, not as a current measurement. Gartner via Infosecurity Magazine, “Predicts 2022: Consolidated Security Platforms Are the Future,” accessed 2026-06-16. https://www.infosecurity-magazine.com/white-papers/prm/predicts-2022-consolidated/ ↩

14. ~61% of CISOs prefer single-vendor SASE in principle while a majority deploy two-vendor in practice; Fortinet and Cato named Leaders in the 2025 Gartner Magic Quadrant for SASE Platforms (Cato citing ~2,500 active enterprise platform customers). Gartner SASE quadrant analysis summary, accessed 2026-06-16, https://sase.cloud/guides/gartner-sase-magic-quadrant-analysis ; Fortinet, “2025 Gartner Magic Quadrant for SASE Platforms,” accessed 2026-06-16, https://www.fortinet.com/resources/analyst-reports/gartner-magic-quadrant-sase ↩↩

15. VPN-to-ZTNA displacement cycle in late innings, with a majority of organizations reported as actively replacing VPNs with ZTNA in 2026. openPR / market report, “Zero Trust Network Access Cybersecurity Market,” accessed 2026-06-16. https://www.openpr.com/news/4488317/zero-trust-network-access-cybersecurity-market-to-reach ↩

16. Non-human identities (service accounts, API keys, machine tokens, AI agents) outnumber human identities in many enterprises by reported ratios of 40:1 to over 100:1, growing >40% year-on-year. Portnox, “AI Agent Access Management,” accessed 2026-06-16. https://www.portnox.com/cybersecurity-101/artificial-intelligence/ai-agent-access-management-controlling-what-autonomous-agents-can-do/ ↩

17. Zscaler’s Zenith Live (Las Vegas) agentic-AI announcement on 2026-06-09 — AI Broker for agent-to-agent (MCP / A2A) traffic with an Agent Registry, and an AI Access Graph mapping identity-application-data lineage — positioning ZTNA toward a machine-identity control plane. Zscaler, “Zscaler Unveils New Product Innovations to Secure Agentic AI,” 2026-06-09, accessed 2026-06-16. https://www.zscaler.com/press/zscaler-unveils-new-product-innovations-secure-agentic-ai ↩

18. Netskope IPO on Nasdaq (ticker NTSK) on 2025-09-18, raising ~USD 908M, pricing at USD 19 (top of range) and closing ~18% up at a ~USD 8.6B market capitalization; ARR ~USD 707M (up 33%) with a net loss of ~USD 170M for the period. CNBC, “Netskope soars 18% on first day of trading, reaches $8.6 billion market cap,” 2025-09-18, accessed 2026-06-16. https://www.cnbc.com/2025/09/18/netskope-ipo-stock-nasdaq-ntsk.html ↩

19. U.S. federal civilian zero-trust-architecture mandates name identity-aware, per-resource access (the ZTNA model) as the target end state, pulling the public sector onto modern edge platforms on a regulatory timetable. CISA Zero Trust Maturity Model context as referenced in ZTNA market drivers, openPR, “Zero Trust Network Access Cybersecurity Market,” accessed 2026-06-16. https://www.openpr.com/news/4488317/zero-trust-network-access-cybersecurity-market-to-reach ↩

20. Data-residency and sovereign-cloud obligations make the location of traffic inspection a compliance question, favoring SSE platforms able to guarantee in-region enforcement points. Mordor Intelligence, “Secure Access Service Edge (SASE) Market” (regional / regulatory drivers and geography segmentation), accessed 2026-06-16. https://www.mordorintelligence.com/industry-reports/global-secure-access-service-edge-market ↩

21. Zscaler Private Access (ZPA) product page, hero “Secure Private Access with ZTNA” and subhead “Extend fast, secure, and reliable private app access for all users from any device or location.” https://www.zscaler.com/products-and-solutions/zscaler-private-access (accessed 2026-06-16). ↩

22. Zscaler Private Access product page, supporting pillar: “Zscaler Private Access (ZPA) offers seamless zero trust connectivity for all users, with AI-powered user-to-app segmentation and context-aware policies.” https://www.zscaler.com/products-and-solutions/zscaler-private-access (accessed 2026-06-16). ↩

23. Zscaler acquisition of Red Canary (managed detection and response, MDR), completed 2025-08-01, for ~$651.4M (the 10-Q purchase consideration; the deal was signed at ~$680M on 2025-05-27), extending Zscaler beyond pure SSE into the SOC/MDR adjacency (cross-references Front 5).

https://www.globenewswire.com/news-release/2025/08/01/3125824/0/en/Zscaler-Completes-Acquisition-of-Red-Canary-to-Accelerate-Innovations-in-Agentic-AI-driven-Security-Operations.html (accessed 2026-06-16). ↩

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

25. Netskope homepage, hero positioning line "Netskope: modern security and networking for the cloud and AI era"; portfolio spans SSE, CASB, SSPM/DSPM, FWaaS, private access. https://www.netskope.com/ (accessed 2026-06-16). ↩↩

26. Netskope completed its IPO on Nasdaq in September 2025, raising ~$908M (47.8M shares at $19) at a valuation of ~$8.6B; ticker NTSK. https://www.securityweek.com/netskope-raises-over-908-million-in-ipo/ ; https://www.techzine.eu/news/security/134756/netskope-reaches-valuation-of-8-6-billion-after-ipo/ (accessed 2026-06-16). ↩

27. Netskope H1 2025 reporting: ARR ~$707M; net loss ~$170M for the half (unprofitable, growth-over-margin posture). https://www.securityweek.com/netskope-raises-over-908-million-in-ipo/ (accessed 2026-06-16). ↩

28. Cato Networks homepage, platform descriptor "World's Leading Single-Vendor SASE Platform" and pillar "One Platform. Start Anywhere. Grow Everywhere."; current hero "From CVE to Protection in Minutes" / "Agentic defense beyond time-to-patch. Cloud-delivered at machine speed." https://www.catonetworks.com/ (accessed 2026-06-16). ↩↩

29. Cato Networks homepage, architecture statement: "Cato's SASE platform converges networking, security, and access into a single, global, AI-powered cloud service." https://www.catonetworks.com/ (accessed 2026-06-16). ↩

30. Cato Networks extended its Series G to ~$409M total at a valuation of more than $4.8B (over $1B raised lifetime); ARR run-rate ~$350M (+43% YoY); 2026 Fortune Cyber 60 (third year); IPO discussed but postponed toward late 2026+. https://www.prnewswire.com/il/news-releases/cato-networks-raises-359-million-at-a-valuation-of-more-than-4-8-billion-302494283.html (accessed 2026-06-16). ↩

31. Cloudflare One (Zero Trust) page, hero "The agile SASE platform" and tagline "Connect and protect your workforce, AI agents, and infrastructure"; pillars include "Identity-first zero trust access for every employee, contractor, and AI agent," "First SASE platform to secure connections to MCP servers," and "First SASE platform with post-quantum encryption across the full stack." https://www.cloudflare.com/sase/ (accessed 2026-06-16). ↩↩

32. Cloudflare One page, network-reach pillars "SASE architecture unified by design — on a global connectivity cloud" and "Cloudflare delivers full SASE from 300+ cities — ›3× more than other SASE vendors." https://www.cloudflare.com/sase/ (accessed 2026-06-16). ↩

33. Cloudflare Q1 2026 (period ended 2026-03-31): revenue ~$639.8M (+34% YoY), ~$4.2B cash, ~$84.1M free cash flow; third consecutive year in the Gartner SSE Magic Quadrant; announced ~20% workforce reduction (1,100+ roles, AI-first restructuring) with ~$140-150M restructuring charges. https://www.tikr.com/blog/cloudflare-q1-2026-34-revenue-growth-but-announces-20-workforce-reduction (accessed 2026-06-16). ↩

34. Forcepoint homepage, hero "AI Moves Fast. Your Data Shouldn't Move Uncontrolled." and tagline "Secure data everywhere from a single platform." https://www.forcepoint.com/ (accessed 2026-06-16). ↩

35. Forcepoint homepage, pillars "AI Is Only as Secure as Your Data," "The Most Advanced Data Classification Available," and "Protect sensitive data across AI tools, cloud apps, web, email, endpoint and network." https://www.forcepoint.com/ (accessed 2026-06-16). ↩

36. Francisco Partners acquired the commercial Forcepoint business from Raytheon in January 2021; TPG acquired the Forcepoint government business (G2CI) for ~$2.45B, a deal that closed 2023-10-02, leaving the commercial SSE entity as a separate PE-held company. https://www.cybersecuritydive.com/news/tpg-acquires-

forcepoint/686007/ (accessed 2026-06-16). ↩

37. Versa Networks homepage, hero "Extend SASE to every part of your network with VersaONE" and tagline "Universal SASE protects and connects every part of your business — from headquarters to branch, cloud to data center, and every user and device in between." https://versa-networks.com/ (accessed 2026-06-16). ↩

38. Versa Networks homepage, platform pillar "A unified platform with one console, one policy, one data lake, and one OS"; VersaAI framing "AI FOR SASE" / "SASE FOR AI." https://versa-networks.com/ (accessed 2026-06-16). ↩

39. Versa Networks' latest verifiable round is a $120M pre-IPO financing led by BlackRock, October 2022 (~$632M raised lifetime); the signaled public listing has not been realized in the years since. Stated plainly as 2022-vintage; no implication of recent capital or imminent IPO. https://versa-networks.com/news/2022/versa-networks-secures-120m-financing-in-pre-ipo-round-led-by-blackrock-to-capitalize-on-rapidly-growing-sase-market/ (accessed 2026-06-16). ↩

40. Tailscale homepage, hero "The best secure connectivity platform for the AI era" and tagline "A Zero Trust identity-based connectivity platform that replaces your legacy VPN, SASE, and PAM." https://tailscale.com/ (accessed 2026-06-16). ↩

41. Tailscale homepage, pillars "Remote access for your global team," "Infrastructure access to wherever your resources live, including Kubernetes clusters," and "Easy, secure, identity-based access to anything." https://tailscale.com/ (accessed 2026-06-16). ↩

42. Tailscale raised a $160M Series C in April 2025 (led by Accel); acquired Border0 (privileged access management) in March 2026, extending the platform from ZTNA into PAM. https://tailscale.com/blog/series-c ; https://www.pymnts.com/acquisitions/2026/tailscale-simplifies-secure-access-with-border0-acquisition/ (accessed 2026-06-16). ↩

43. Twingate homepage, hero "Security, Performance, Simplicity. Pick Three." and value proposition "Identity-based access for users, services, and AI agents that deploys in minutes, scales to every resource, and finally lets you retire your VPN." https://www.twingate.com/ (accessed 2026-06-16). ↩

44. Twingate homepage, pillars "Zero Trust with No Boundaries," "Protect Every Click," and "Democratize Privileged Access." https://www.twingate.com/ (accessed 2026-06-16). ↩

45. Twingate's most recent verifiable round is a $42M Series B dated 2022-04-14 (~$67M raised lifetime); no newer round surfaced in the bounded scan. Stated plainly as 2022-vintage; no implication of recent capital. https://tracxn.com/d/companies/twingate/__c35wWrBcnX8V7hJ-VfrPl0YSjJ17izwNusJlyDvgjyA/funding-and-investors (accessed 2026-06-16). ↩

46. Cato Networks, "Cato Networks Raises $359 Million at a Valuation of More Than $4.8 Billion," 2025, https://www.prnewswire.com/news-releases/cato-networks-raises-359-million-at-a-valuation-of-more-than-4-8-billion-302494283.html (accessed 2026-06-16); Cato Networks, "Cato Surpasses $350 Million ARR with 43% YoY Growth in 2025," https://www.catonetworks.com/news/cato-surpasses-350-million-arr-with-43-yoy-growth-in-2025/ (accessed 2026-06-16). Series G totaled ~$409M (initial round plus extension) at a valuation above $4.8B; ARR surpassed $350M at 43% YoY growth; IPO deferred. ↩

47. SecurityWeek, "Netskope Raises Over $908 Million in IPO," 2025, https://www.securityweek.com/netskope-raises-over-908-million-in-ipo/ (accessed 2026-06-16). Netskope (NASDAQ: NTSK) IPO'd on Nasdaq in September 2025, raising ~$908M at ~$8.6B valuation; first-half 2025 ARR ~$707M; ~$1.5B raised pre-IPO. ↩

48. Microsoft Learn, "Microsoft Entra Internet Access" / "Global Secure Access," 2026, https://learn.microsoft.com/en-us/entra/global-secure-access/concept-internet-access (accessed 2026-06-16). Entra Internet Access and Entra Private Access form Microsoft's Global Secure Access SSE family; Defender for Cloud Apps serves as the cloud access security broker. Microsoft's primary characterization in this report is in Front 5; here it appears as a cross-front SSE play via Entra Internet Access, not as a Front 6 contender. ↩

49. Palo Alto Networks, "Prisma Access," product page, https://www.paloaltonetworks.com/sase/access (accessed 2026-06-16); Reuters, Palo Alto Networks–CyberArk acquisition close, 2026, https://www.reuters.com/business/palo-alto-networks-completes-cyberark-acquisition-2026/ (accessed 2026-06-16). Prisma Access is Palo Alto Networks' SSE layer; the ~$25B CyberArk acquisition closed 2026-02-11. Palo Alto Networks' primary characterization in this report is in Front 5; here it appears as a cross-front SSE play via Prisma Access. ↩

50. Cisco, "Cisco Umbrella" and "Cisco Hypershield" product pages, https://umbrella.cisco.com/ (accessed 2026-06-16); https://www.cisco.com/site/us/en/products/security/hypershield/index.html (accessed 2026-06-16). Cisco carries Umbrella, Duo, and Hypershield into existing network accounts as an SSE-adjacent bundle. Cisco's primary characterization in this report is in Front 5 (its Splunk-era platform); here it appears as a cross-front SSE play. ↩

51. Cross-front primary-slot note: Microsoft, Palo Alto Networks, and Cisco are analyzed as primary contenders in Front 5 (Detection & Response). In Front 6 they appear only as §6.4 Plays exerting bundle pressure on the SSE pure-plays, named by their SSE-specific product families (Entra Internet Access, Prisma Access, Umbrella/Duo/Hypershield), per the report's cross-front primary-slot map. ↩

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

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

54. Cross-front note: the detection-and-response incumbents whose managed-service revenue Zscaler's Red Canary acquisition contests (including CrowdStrike Falcon Complete and Microsoft's managed Defender services) are characterized primarily in Front 5; this Play references that boundary rather than re-grading those vendors here. ↩

55. Tailscale, "Series C," April 2025, https://tailscale.com/blog/series-c (accessed 2026-06-16); PYMNTS, "Tailscale Simplifies Secure Access With Border0 Acquisition," 2026, https://www.pymnts.com/acquisitions/2026/tailscale-simplifies-secure-access-with-border0-acquisition/ (accessed 2026-06-16). $160M Series C led by Accel, April 2025; Border0 (privileged access management) acquired March 2026. ↩

56. Twingate (private): $42M Series B, April 2022, ~$67M total raised; no comparable recent capital event on the public record. Tracxn, Twingate funding and investors, https://tracxn.com/d/companies/twingate/__c35wWrBcnX8V7hJ-VfrPl0YSjJ17izwNusJlyDvgjyA/funding-and-investors (accessed 2026-06-16). Print the year, no recent-capital implication. ↩

57. Netskope (NASDAQ: NTSK): IPO on Nasdaq September 2025, raised ~$908M at ~$8.6B valuation; ~$1.5B raised pre-IPO; first-half 2025 ARR ~$707M. SecurityWeek, "Netskope Raises Over $908 Million in IPO," 2025, https://www.securityweek.com/netskope-raises-over-908-million-in-ipo/ (accessed 2026-06-16). ↩

58. Zscaler (NASDAQ: ZS): acquired Red Canary (MDR) for ~$651.4M, completed 2025-08-01; fiscal Q3 2026 ARR ~$3,525M, revenue ~$850M (+25% YoY). Form 10-Q, period ended 2026-04-30, https://www.sec.gov/Archives/edgar/data/0001713683/000171368326000096/zs-20260430.htm (accessed 2026-06-16). ↩

59. Cloudflare (NYSE: NET): Q1 2026 revenue $639.8M (+34% YoY); ~$4.2B cash and equivalents. Cloudflare, Form 10-Q, period ended 2026-03-31, https://www.sec.gov/Archives/edgar/data/0001477333/000147733326000038/cloud-20260331.htm (accessed 2026-06-16). ↩

60. Cloudflare (NYSE: NET): on May 7, 2026 announced a plan to accelerate its shift to an agentic AI-first operating model, reducing workforce by ~20% (~1,100 roles), with estimated restructuring charges of $140–150M (cash severance/benefits $105–110M; non-cash share-based vesting $35–40M), majority incurred in fiscal Q2 2026. Cloudflare, Form 8-K, fiscal Q1 2026, https://www.sec.gov/Archives/edgar/data/0001477333/000147733326000033/q126exhibit991.htm (accessed 2026-06-16); TechCrunch, "Cloudflare says AI made 1,100 jobs obsolete, even as revenue hit a record high," 2026-05-08, https://techcrunch.com/2026/05/08/cloudflare-says-ai-made-1100-jobs-obsolete-even-as-revenue-hit-a-record-high/ (accessed 2026-06-16). This is a strong-growth company restructuring to an AI-first model, not a distressed company; it is noted as a cited public corporate event, not a casualty label. ↩

61. Cato Networks (private): $409M Series G (initial round plus extension) at a valuation above $4.8B in 2025, led by new investors Vitruvian Partners and ION Crossover Partners with existing investors including Lightspeed Venture Partners; more than $1B raised to date; IPO deferred. Cato Networks, "Cato Networks Raises $359 Million at a Valuation of More Than $4.8 Billion," 2025, https://www.prnewswire.com/news-releases/cato-networks-raises-359-million-at-a-valuation-of-more-than-4-8-billion-302494283.html (accessed 2026-06-16). ↩

62. Tailscale (private): $160M Series C, April 2025, led by Accel; acquired Border0 (PAM) March 2026. Tailscale, "Series C," https://tailscale.com/blog/series-c (accessed 2026-06-16); PYMNTS, https://www.pymnts.com/acquisitions/2026/tailscale-simplifies-secure-access-with-border0-acquisition/ (accessed 2026-06-16). ↩

63. Versa Networks (private): last round a $120M pre-IPO financing led by BlackRock, October 2022; ~$632M raised to date; IPO unrealized. No recent capital event; print the year, no recent-capital or imminent-IPO implication. Versa Networks, "Versa Networks Secures $120M Financing in Pre-IPO Round Led by BlackRock," 2022, https://versa-networks.com/news/2022/versa-networks-secures-120m-financing-in-pre-ipo-round-led-by-blackrock-to-capitalize-on-rapidly-growing-sase-market/ (accessed 2026-06-16). ↩

64. Netskope (Nasdaq: NTSK) IPO 2025-09-18, ~$908.2M raised, ~$8.6–8.79B debut valuation; Q1 fiscal 2027 (quarter ended 2026-04-30; Netskope's fiscal year ends January 31) ARR $845M (+29% YoY), revenue $202M (+28% YoY), customers paying $100K+ ARR grew 23% YoY to ~1,600; platform bundles DLP alongside CASB/SSPM/DSPM. CNBC, "Netskope soars 18% on first day of trading, reaches $8.6 billion market cap," and Netskope Q1 fiscal 2027 earnings coverage, accessed 2026-06-16. https://www.cnbc.com/2025/09/18/netskope-ipo-stock-nasdaq-ntsk.html ; https://finance.yahoo.com/markets/stocks/articles/netskope-inc-ntsk-q1-2026-050038565.html ↩↩↩↩↩

65. Zscaler (NASDAQ: ZS), Form 10-Q for the period ended 2026-04-30 (fiscal Q3 2026): ARR ~$3,525M (+25% YoY), revenue ~$850M (+25% YoY); DLP bundled inside the Zero Trust Exchange. https://www.sec.gov/Archives/edgar/data/0001713683/000171368326000096/zs-20260430.htm (accessed 2026-06-16). ↩↩↩↩

66. SSE platforms ship DLP as a bundled module of the broader Security Service Edge bundle (SWG, CASB, ZTNA, FWaaS) reaching the buyer inside a platform already purchased for secure web gateway and zero-trust access, rather than as a standalone evaluation. Netskope platform overview (DLP/CASB/SSPM/DSPM) and Zscaler product portfolio, accessed 2026-06-16. https://www.netskope.com/products ; https://www.zscaler.com/products-and-solutions ↩↩

67. Tailscale raised a $160M Series C (April 2025, led by Accel) and announced its first acquisition, privileged-access-management startup Border0, on 2026-03-17, building out PAM and zero-trust access capabilities; Bloomberg framed the deal around AI agents requiring per-resource server access. Bloomberg, "Canada Cyber Startup Tailscale Buys Border0 as AI Agents Spill Onto Servers," accessed 2026-06-16. https://www.bloomberg.com/news/articles/2026-03-17/canada-cyber-startup-tailscale-buys-border0-as-ai-agents-spill-onto-servers ; BetaKit, "Tailscale makes first acquisition with Border0 purchase," https://betakit.com/tailscale-makes-first-acquisition-with-border0-purchase/ ↩↩↩

68. Incumbent identity-access acquisition cluster aimed at the machine-and-agent access problem: Palo Alto Networks completed its ~$25B acquisition of CyberArk on 2026-02-11 (regulatory clearances in U.S., EU, UK, Israel); CrowdStrike acquired identity-security firm SGNL for $740M (January 2026); Cisco agreed to acquire non-human-identity vendor Astrix for a reported ~$400M (May 2026); Microsoft shipped Entra Agent ID giving AI agents first-class identities. GovCon Wire, "Palo Alto Networks Closes $25B Acquisition of CyberArk," accessed 2026-06-16. https://www.govconwire.com/articles/palo-alto-networks-cyberark-25b-acquisition ↩↩

69. ZTNA enforces per-application, continuously-verified access — the named enforcement primitive for an AI agent that must reach exactly one authorized resource and no more; non-human identities (service accounts, API keys, machine tokens, AI agents) now outnumber human identities in many enterprises and are among the fastest-growing attack surfaces per NIST. Exabeam, "ZTNA Solutions: Key Capabilities and 9 Options to Know in 2026," accessed 2026-06-16. https://www.exabeam.com/explainers/zero-trust/ztna-solutions-key-capabilities-and-9-options-to-know/ ↩↩

70. Cato Networks surpassed $350M ARR with 43% YoY growth in 2025 and raised a $409M Series G at a valuation above $4.8 billion, keeping its IPO deferred. Cato Networks, "Cato Networks Raises $359 Million at a Valuation of More Than $4.8 Billion," accessed 2026-06-16. https://www.prnewswire.co.uk/news-releases/cato-networks-raises-359-million-at-a-valuation-of-more-than-4-8-billion-302494248.html ; "Cato Networks Surpasses $350 Million ARR with 43% YoY Growth in 2025," https://www.catonetworks.com/news/cato-surpasses-350-million-arr-with-43-yoy-growth-in-2025/ ↩↩↩↩

71. Cato Networks named to the 2026 Fortune Cyber 60 list for a third consecutive year — a cohort of venture-backed startups that have not had an IPO, acquisition, or other significant exit. Cato Networks / PR Newswire, "Cato Networks Named to 2026 Fortune Cyber 60 List for Third Consecutive Year," accessed 2026-06-16. https://www.prnewswire.com/news-releases/cato-networks-named-to-2026-fortune-cyber-60-list-for-third-consecutive-year-302599099.html ↩↩↩

72. Netskope (NASDAQ: NTSK) public since September 2025 and Zscaler (NASDAQ: ZS) trading as a scaled public SSE platform give best-of-breed assemblers two fully public SSE reference points. See [64] and [65]. ↩↩

73. Zscaler completed its acquisition of managed-detection-and-response house Red Canary (completed 2025-08-01) for ~$651.4M, extending Zscaler beyond pure SSE into the SOC/MDR adjacency. Zscaler press release, accessed 2026-06-16. https://www.globenewswire.com/news-release/2025/08/01/3125824/0/en/Zscaler-Completes-Acquisition-of-Red-Canary-to-Accelerate-Innovations-in-Agentic-AI-driven-Security-Operations.html ↩

74. Cloudflare (NYSE: NET) Form 8-K (FY2026) disclosed a workforce reduction of approximately 1,100 people (~20% of headcount) to accelerate an agentic-AI-first operating model, with charges of $140–150M; co-founders stated explicitly it was not a cost-cutting exercise or a performance assessment. SecurityWeek, "Cloudflare Lays Off 1,100 Employees in AI-Driven Restructuring," and Cloudflare Form 8-K FY2026, accessed 2026-06-16. https://www.securityweek.com/cloudflare-lays-off-1100-employees-in-ai-driven-restructuring/ ; https://www.sec.gov/Archives/edgar/data/0001477333/000147733326000033/q126exhibit991.htm ↩↩

75. Cloudflare named a Visionary in the 2025 Gartner Magic Quadrant for SASE Platforms. Cloudflare blog, "Cloudflare recognized as a Visionary in 2025 Gartner Magic Quadrant for SASE Platforms," accessed 2026-06-16. https://blog.cloudflare.com/cloudflare-sase-gartner-magic-quadrant-2025/ ↩↩

76. Netskope (NASDAQ: NTSK) and Zscaler (NASDAQ: ZS) investor relations — earnings transcripts and 10-Q filings disclosing data-security (DLP/DSPM) attach as a platform growth driver. SEC EDGAR, accessed 2026-06-16. https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=0001713683 (Zscaler) ; Netskope IR https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&company=netskope&type=10-Q ↩

77. SSE/ZTNA leader product-page hero snapshots and Zscaler/Netskope earnings transcripts disclosing named non-human-identity / agent-access SKUs as growth drivers. Zscaler Zenith Live 2026 AI Broker / Agent Registry / AI Access Graph announcements and vendor product pages, accessed 2026-06-16. https://www.zscaler.com/products-and-solutions ↩

78. Acquirer SEC filings (Form 8-K) and vendor product announcements documenting closing and integration of the identity-access acquisition cluster (PANW/CyberArk, CRWD/SGNL, Cisco/Astrix). GovCon Wire (PANW/CyberArk close) and acquirer investor relations, accessed 2026-06-16. https://www.govconwire.com/articles/palo-alto-networks-cyberark-25b-acquisition ↩

79. Cato Networks IPO-or-enterprise trajectory — SEC EDGAR S-1 filings and named-outlet (Calcalist / SecurityWeek / Bloomberg) enterprise coverage. Calcalist, "Cato Networks hits $350 million revenue run rate amid IPO uncertainty," accessed 2026-06-16. https://www.calcalistech.com/ctechnews/article/rjf7exsube ↩

80. Gartner Magic Quadrant for SASE Platforms / Security Service Edge refresh and vendor placement announcements. Cloudflare 2025 SASE Platforms quadrant placement (Visionary) as the prior-cycle baseline, accessed 2026-06-16. https://blog.cloudflare.com/cloudflare-sase-gartner-magic-quadrant-2025/ ↩

# Disclosures

### DISCLOSURE.

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

### AFFILIATION.

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

### NOT ADVICE.

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