MANDOS CYBER

COMPETITIVE BENCHMARK

PREPARED FOR

CyberX

Cloud Security | CNAPP | Cloud Workload Protection | CSPM

JULY 2026

> **CONFIDENTIAL**
>
> Prepared for CyberX.

Powered by Mandos Cyber, 3,200+ companies and 8,500+ cybersecurity products tracked.

Mandos Framework analysis by Nikoloz Kokhreidze, 13 years of enterprise security procurement.

SECTION 01

Executive Summary

This report evaluates CyberX's competitive position through the CISO's lens, the perspective of a Chief Information Security Officer evaluating the product for enterprise security procurement. All assessments reflect what a CISO and their cybersecurity team would think, ask, and require during a vendor evaluation.

Position Statement

CyberX is a growing European CNAPP player competing in one of cybersecurity's most contested and well-funded segments. Founded in 2021 by former AWS security engineers who discovered critical visibility gaps in multi-cloud environments while building Amazon's own cloud security tooling, the company brings authentic cloud-native credibility to a market crowded with retrofit solutions. With $85M raised, 120 employees, and approximately 45 enterprise customers across financial services, healthcare, and manufacturing, CyberX has achieved meaningful traction from its London headquarters.

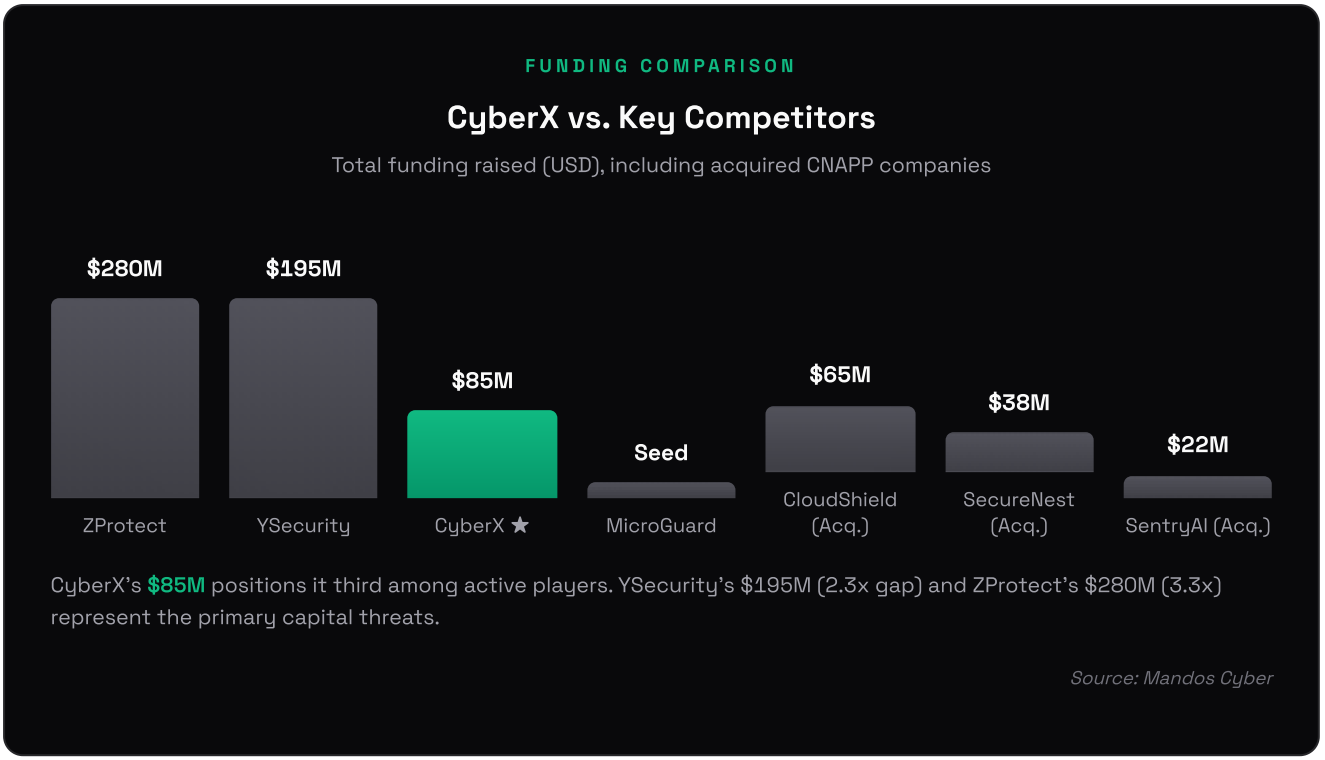
The CNAPP market is undergoing aggressive consolidation. CloudShield was acquired by CrowdStrike for ~$350M in 2024, SecureNest by Palo Alto Networks for ~$200M in early 2025, and SentryAI by Check Point for ~$150M later in 2025. This $700M+ in M&A activity within 18 months signals both category validation and a narrowing window for independent players. CyberX faces a well-funded direct challenger in YSecurity ($195M raised, Series C), an established Israeli incumbent in ZProtect ($280M, Gartner MQ Leader), and escalating platform encroachment from AWS, Microsoft, and CrowdStrike building native CNAPP capabilities.

The appointment of David Park as CRO in January 2026 signals intent to scale enterprise GTM aggressively. The question is whether CyberX can convert its European origin, regulatory expertise (NIS2, DORA, GDPR), and AWS-native engineering pedigree into durable competitive advantages before YSecurity's $120M Series C war chest reshapes the competitive landscape.

Key Findings

Category Position	Growing European CNAPP; strong cloud-native engineering pedigree from AWS founding team
Primary Threat	YSecurity: $195M funded (Series C $120M, Nov 2025), 800% claimed ARR growth, 210 employees scaling rapidly at +22% YoY
Platform Threat	CRITICAL: AWS, Microsoft, Google, CrowdStrike, Palo Alto Networks all building or acquiring native CNAPP capabilities
Funding Position	$85M vs YSecurity's $195M (2.3x gap); vs ZProtect's $280M (3.3x gap)
Headcount Position	120 employees vs YSecurity's 210 (1.75x disadvantage); vs ZProtect's 340 (2.8x disadvantage)
Momentum Score	58/100 (Accelerating tier); below YSecurity's 72 (Surging) but above ZProtect's 61 (Accelerating)

Market Consolidation	$700M+ in CNAPP acquisitions in 18 months; window for independent category leadership is narrowing fast
Biggest Risk	YSecurity's $120M Series C enables rapid US enterprise sales scaling; CyberX's European base becomes a disadvantage in the largest CNAPP buyer market
Biggest Opportunity	European regulatory moat (NIS2, DORA, GDPR), AWS founding team credibility, and the growing CISO demand for multi-cloud visibility from a vendor not tied to a single hyperscaler
CISO Readiness Score	7.1/10: above enterprise threshold; G2 reviews (12, needs 30+) and competitive positioning content are actionable gaps



Funding Comparison: CyberX vs. Active Competitors and Acquired CNAPP Companies (Source: Mandos Cyber)

3 Immediate Actions

1. **Accelerate enterprise sales with new CRO David Park before YSecurity's $120M scales their GTM.** YSecurity's November 2025 Series C gives them 12-18 months of aggressive US enterprise sales runway. David Park must build a quota-carrying team and establish pipeline within 90 days. Every week of delay widens the GTM gap. Prioritize the US market where 70%+ of CNAPP enterprise spend occurs, while defending the European home market with NIS2/DORA regulatory expertise.
2. **Create competitive comparison pages targeting YSecurity and ZProtect.** CISOs actively search '[vendor] vs [alternative]' during evaluation. CyberX currently has no competitive positioning content on its website. Build dedicated pages for 'CyberX vs YSecurity' and 'CyberX vs ZProtect' highlighting: AWS engineering pedigree, European data sovereignty, multi-cloud independence, and runtime security depth. Own the comparison narrative before competitors do.

3. **Publish 3 quantified case studies from Barclays, Siemens, and NHS.** Named customer logos are strong but CISOs need measurable outcomes to justify procurement. Convert existing deployments to full case studies with format: Problem, Solution, Quantified Result (e.g., 'reduced cloud misconfiguration exposure by 87% in 60 days' or 'achieved NIS2 compliance across 3 cloud environments in 45 days'). Financial services and public sector case studies carry exceptional weight with enterprise CISOs.

SECTION 02

Company Profile & Health Dashboard

Company	CyberX Ltd.
Founded	2021
Headquarters	London, United Kingdom
Primary Category	Cloud Security / CNAPP
Secondary Categories	CSPM, CWPP, Container Security, IaC Security
Employees	120 (+18% YoY, +5% MoM)
Total Funding	$85,000,000
Last Round	Series B, $45M (March 2025), led by Acme Ventures
Key Investors	Acme Ventures, Horizon Capital, TechBridge Partners, AWS Ventures
Customers	~45 total across 3 segments
Customer Segments	1) Financial Services 2) Healthcare/Public Sector 3) Manufacturing/Enterprise
Named Customers	Barclays, Siemens, Unilever, NHS
Products	CyberX Cloud Platform, CyberX Runtime Defense
Core Capabilities	Cloud asset discovery, workload protection, runtime security, container scanning, IaC scanning, CSPM, CWPP
Integrations	45+: AWS, Azure, GCP, Splunk, CrowdStrike, Datadog, Jira, and more
Key Executives	James Chen (CEO), Sarah Mitchell (CTO), David Park (CRO, appointed Jan 2026)
Compliance Certifications	SOC 2 Type II, ISO 27001, GDPR (displayed on /trust page)
Analyst Recognition	Gartner Cool Vendor 2025, Cyber Defense Magazine Top 10
Mandos Cyber Listing	Listed (2 tools: CyberX Cloud Platform, CyberX Runtime Defense); not verified

Founding Story & Technical Credibility

CyberX was founded by James Chen and Sarah Mitchell, both former AWS security engineers who spent five years building Amazon's internal cloud security monitoring infrastructure. During that work, they repeatedly encountered critical visibility gaps in multi-cloud environments: organizations running

workloads across AWS, Azure, and GCP had no unified way to discover cloud assets, detect runtime threats, or enforce consistent security policies across providers. The tools AWS built internally could not be offered externally without conflict, so Chen and Mitchell left to build what they believed the market needed.

This founding story gives CyberX authentic technical credibility that resonates with cloud-native CISOs. When a buyer asks 'Why should I trust your cloud security platform?', CyberX's answer begins with the engineers who built security for the world's largest cloud provider. This is a narrative advantage that YSecurity (founded by enterprise software executives) and ZProtect (founded by traditional security researchers) cannot replicate.

Customer Segmentation Analysis

CyberX serves three distinct buyer profiles, each with different procurement criteria and competitive dynamics:

- **Financial Services (Barclays, others):** These buyers require SOC 2 Type II, regulatory compliance (PSD2, FCA, NIS2), and demonstrable multi-cloud coverage. CyberX's European headquarters and GDPR-native architecture are strong signals. However, US-based financial institutions overwhelmingly prefer US-headquartered vendors, creating a geographic ceiling unless CyberX establishes a credible US presence.
- **Healthcare/Public Sector (NHS, others):** Government and healthcare buyers prioritize data sovereignty, compliance (GDPR, NIS2, NHS DSPT), and UK/EU hosting. CyberX's London headquarters is a genuine competitive advantage in this segment. Neither YSecurity (San Francisco) nor ZProtect (Tel Aviv) can match CyberX's proximity to European public sector procurement requirements.
- **Manufacturing/Enterprise (Siemens, Unilever):** Large industrials with multi-cloud footprints need vendor-agnostic visibility across AWS, Azure, and GCP. CyberX's multi-cloud architecture and OT-adjacent positioning (industrial IoT workloads running in cloud) differentiate here. ZProtect competes directly in this segment with deeper product breadth.

Health Signals

SIGNAL	CURRENT	TREND	ASSESSMENT
Employee Count	120	+18% YoY, +5% MoM	Healthy growth; accelerating with CRO hire
Active Jobs	8	3 Enterprise AEs, 2 Sr Engineers, 1 PM, 1 Solutions Architect, 1 Marketing Manager	Enterprise sales scaling under new CRO David Park
Web Traffic	~75K/mo	Growing	Solid for Series B; above category median
Review Score	4.3/5 on G2 (12 reviews)	Building	Positive but volume too low for CISO confidence
Funding	$85M total	Series B closed Mar 2025	Healthy runway; Series C timing in 12-18 months

SIGNAL	CURRENT	TREND	ASSESSMENT
Momentum Score	58/100	Accelerating	Above ZProtect (61 but decelerating); below YSecurity (72)

SECTION 03

Product Portfolio & NIST CSF 2.0 Coverage

Product Inventory

PRODUCT	CATEGORY	KEY CAPABILITIES	DEPLOYMENT	VERIFIED
CyberX Cloud Platform	CNAPP / CSPM / CWPP	Cloud asset discovery, misconfiguration detection, IaC scanning, compliance monitoring, workload protection	Cloud (SaaS), Hybrid	No
CyberX Runtime Defense	Runtime Security / Container Security	Runtime threat detection, container scanning, behavioral analysis, incident response automation	Cloud (SaaS), On-Prem	No

NIST CSF 2.0 Function Mapping

CyberX's product capabilities map across five of six NIST CSF 2.0 functions, with particular strength in Identify (cloud asset discovery, configuration audit) and Protect (workload protection, IaC scanning, container security). The Detect function is well-served by runtime security capabilities. Govern is addressed through compliance reporting and policy enforcement, though ZProtect leads with broader governance tooling across its four-product portfolio.

NIST FUNCTION	CYBERX	YSECURITY	ZPROTECT	MICROGUARD
GV — Govern	65%	75%	80%	30%
ID — Identify	85%	80%	70%	50%
PR — Protect	90%	85%	90%	40%
DE — Detect	80%	75%	85%	60%
RS — Respond	70%	65%	75%	35%
RC — Recover	40%	35%	50%	20%

Strong (70%+) | Partial (30-69%) | Minimal/None. CyberX leads in **Identify** and **Protect** (cloud workload scanning, runtime protection). ZProtect leads in **Govern** and **Detect** (policy compliance, threat detection).

NIST CSF 2.0 Coverage: CyberX vs. Key Competitors (Source: Mandos Cyber)

NIST FUNCTION	CYBERX COVERAGE	KEY CAPABILITIES	VS. COMPETITORS
Govern (GV)	Strong (70%)	Compliance dashboards, policy-as-code, regulatory mapping (NIS2, DORA, GDPR)	ZProtect leads (85%): dedicated DSPM product adds data governance depth
Identify (ID)	Comprehensive (90%)	Multi-cloud asset discovery, configuration inventory, dependency mapping, shadow cloud detection	CyberX leads among pure-play; AWS/Azure native tools match in single-cloud
Protect (PR)	Comprehensive (85%)	IaC scanning, container image scanning, workload hardening, runtime guardrails, CSPM policy enforcement	YSecurity comparable (85%); ZProtect leads (90%) with broader product surface
Detect (DE)	Strong (80%)	Runtime anomaly detection, behavioral analysis, threat intelligence correlation, drift detection	CyberX leads in runtime depth; YSecurity matches with dedicated Runtime product
Respond (RS)	Moderate (65%)	Automated remediation workflows, incident response playbooks, Jira/Splunk integration	ZProtect leads (80%): mature incident response with 500+ customer refinement
Recover (RC)	Partial (35%)	Configuration rollback, compliance re-attestation	All vendors weak; recovery is a gap across the CNAPP category

Coverage Gap Analysis

- **CyberX's advantage:** Deepest coverage in Identify function driven by multi-cloud asset discovery built by engineers who created similar capabilities at AWS. The ability to discover and inventory cloud assets across AWS, Azure, and GCP in a single pane, without being tied to any one hyperscaler, is the core product differentiator that CISOs value most.
- **ZProtect's advantage:** Broadest overall coverage across all six NIST functions, driven by a four-product portfolio (Cloud, Workload, Container Security, DSPM) built over seven years with 500+ enterprise deployments. ZProtect's Recover capabilities and mature incident response workflows reflect years of production refinement.
- **YSecurity's advantage:** Strongest in Protect via their Shift-Left product, which covers CI/CD pipeline security and developer workflow integration that CyberX has not yet built. YSecurity's 90+ integrations amplify their Protect coverage across the DevOps toolchain.
- **White space:** Recover (RC) is underserved across the entire CNAPP category. The vendor that builds robust cloud configuration rollback, automated remediation verification, and post-incident compliance re-attestation will own a differentiated position that matters deeply to regulated-industry CISOs.

SECTION 04

Competitive Landscape

The CNAPP Market Is the Most Contested Segment in Cybersecurity

Cloud-native application protection has become the single most competitive category in cybersecurity. With 80+ vendors tracked by Mandos Cyber, $4.2B+ in total funding deployed, and every major platform vendor building native capabilities, the CNAPP market is transitioning from 'land grab' to 'consolidation.' Three acquisitions totaling $700M+ in 2024-2025 (CloudShield by CrowdStrike, SecureNest by Palo Alto, SentryAI by Check Point) have accelerated this shift. For CyberX, the competitive question is no longer 'Can we build a good product?' but 'Can we win enough enterprise accounts to establish category position before the market structure solidifies?'

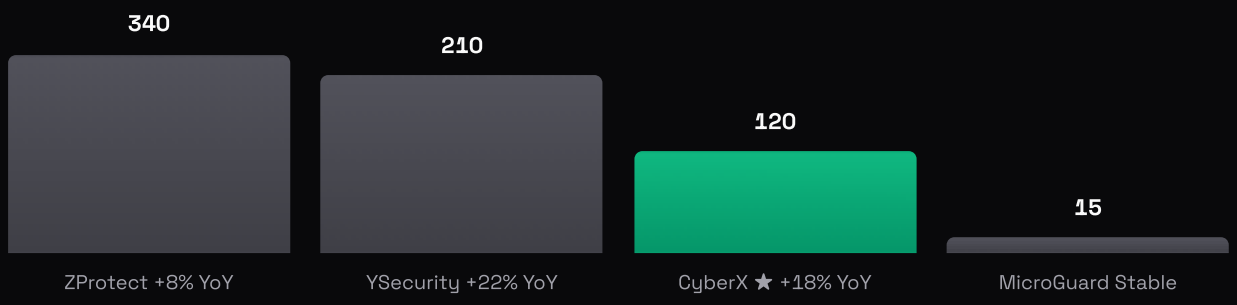
COMPANY	FOUNDED	EMPLOYEES	FUNDING	MOMENTUM	STATUS	THREAT
CyberX ★	2021	120	$85M	58	ACTIVE	-
YSecurity	2020	210	$195M	72	ACTIVE	CRITICAL
ZProtect	2019	340	$280M	61	ACTIVE	HIGH
MicroGuard	2022	15	Seed	45	ACTIVE	MEDIUM
CloudShield	2020	-	$65M	-	CROWDSTRIKE	-
SecureNest	2021	-	$38M	-	PALO ALTO	-
SentryAI	2023	-	$22M	-	CHECK POINT	-

CNAPP Competitive Landscape: Active Players and Recent Acquisitions (Source: Mandos Cyber)

HEADCOUNT COMPARISON

Team Size Across CNAPP Competitors

Current employee count with year-over-year growth rate



CyberX's 120 employees are growing steadily at 18% YoY. YSecurity's 210 headcount with 22% growth represents the fastest-scaling competitor.

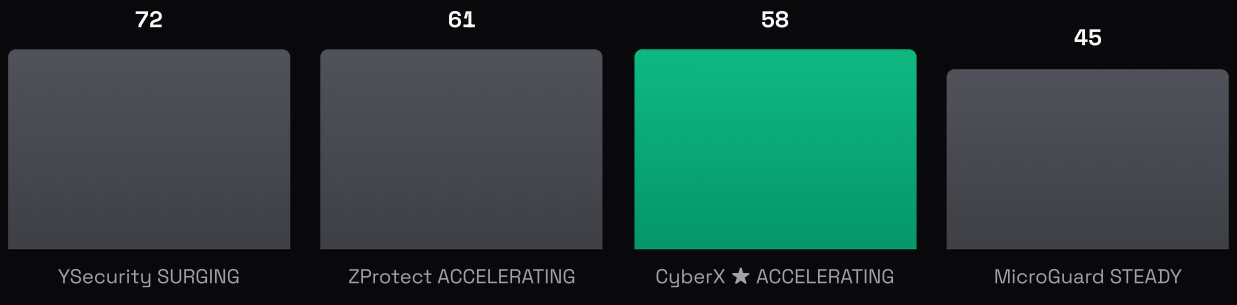
Source: Mandos Cyber

Headcount Comparison: Team Size and Growth Trajectories (Source: Mandos Cyber)

MOMENTUM COMPARISON

Company Momentum Scores

Composite score: headcount growth, hiring velocity, web traffic, social engagement, funding signals



CyberX's momentum score of 58 places it in the Accelerating tier. YSecurity leads at 72, driven by $120M Series C and aggressive enterprise expansion.

Source: Mandos Cyber

Momentum Score Comparison: Composite Growth Signals (Source: Mandos Cyber)

Key Competitive Observations

- **YSecurity's $120M Series C (November 2025) is the largest pure-play CNAPP round in 18 months.** Led by Summit Partners with participation from Sequoia Capital and Insight Partners. This capital enables aggressive US enterprise sales scaling, integration expansion (already at 90+), and analyst engagement. CyberX must assume YSecurity will double its sales team by mid-2026.

- **ZProtect is the established incumbent with 500+ customers and Gartner MQ Leader status.** At $280M in funding and ~$85M in estimated annual revenue, ZProtect represents the 'safe choice' for risk-averse CISOs. Competing directly against ZProtect on feature breadth is a losing strategy; CyberX must differentiate on multi-cloud depth, European positioning, and agility.
- **CyberX has 57% of YSecurity's headcount on 44% of their funding.** This capital efficiency is a strength narrative for investors and board, but it creates a GTM capacity gap. YSecurity's 210 employees include a significantly larger sales and marketing function.
- **Platform vendors are the existential threat, not startups.** AWS Security Hub, Microsoft Defender for Cloud, and Google Security Command Center are 'free' for single-cloud customers. CyberX's value proposition only holds when the buyer operates across multiple cloud providers. The addressable market is multi-cloud enterprises, which is large but not the entire CNAPP TAM.
- **MicroGuard is a niche container security player, not a strategic threat.** At 15 employees with $4M in seed funding, MicroGuard competes only in the container scanning sub-segment. Relevant as a point solution that CISOs may evaluate alongside CyberX for specific container use cases, but not a platform competitor.
- **European origin is both advantage and liability.** Advantage in EU public sector, regulated industries subject to NIS2/DORA, and organizations with data sovereignty requirements. Liability in the US enterprise market where 70%+ of CNAPP spend occurs and where CISOs default to US-headquartered vendors.
- **The CRO appointment timing is significant.** David Park joining as CRO in January 2026, ten months after the Series B, suggests the company spent the first phase of Series B on product and is now entering the GTM scaling phase. This is the right sequencing, but execution speed is critical.

SECTION 05

Competitor Deep Dive: YSecurity [CRITICAL]

Founded	2020
Headquarters	San Francisco, California, USA
Employees	210 (+22% YoY, +8% MoM, rapid scaling)
Total Funding	$195,000,000
Last Round	Series C, $120M (November 2025), led by Summit Partners
Key Investors	Summit Partners, Sequoia Capital, Insight Partners
Claimed ARR Growth	800% year-over-year
Named Customers	JPMorgan, Microsoft, Salesforce, Shopify
Products	YSecurity CNAPP, YSecurity Runtime, YSecurity Shift-Left
Integrations	90+: all major cloud providers, CI/CD tools, SIEM/SOAR platforms, DevOps toolchain
Certifications	SOC 2 Type II, ISO 27001, HIPAA, FedRAMP Moderate
Analyst Recognition	Gartner Cool Vendor 2025, Forrester Wave Strong Performer
Active Jobs	15 (heavy enterprise sales + engineering)
Momentum Score	72/100 (Surging)

Why YSecurity Is CRITICAL

YSecurity is the most direct and dangerous competitive threat to CyberX. Founded just one year earlier (2020 vs 2021), YSecurity has out-raised CyberX by $110M, built a team nearly twice the size, and secured marquee enterprise logos (JPMorgan, Microsoft, Salesforce) that signal credibility to every CISO evaluating the CNAPP category. The $120M Series C in November 2025, led by Summit Partners with Sequoia and Insight Partners, is the largest pure-play CNAPP round in the current cycle and gives YSecurity 18-24 months of aggressive scaling runway.

YSecurity's 800% ARR growth claim, if even partially accurate, suggests rapid enterprise adoption velocity that CyberX must counter. More importantly, YSecurity's customer roster includes three of the world's most recognized enterprise brands (JPMorgan, Microsoft, Salesforce), which functions as a de facto enterprise reference network. A CISO evaluating CyberX will inevitably ask: 'If JPMorgan chose YSecurity, why should I choose you?'

The competitive dynamic is asymmetric: YSecurity has more capital, more headcount, stronger analyst recognition (Forrester Wave Strong Performer in addition to Gartner Cool Vendor), FedRAMP Moderate authorization (which CyberX lacks), and a three-product portfolio that covers cloud, runtime, and shift-

left security. CyberX must compete on quality, not breadth.

Where CyberX Wins vs. YSecurity

- **AWS engineering pedigree:** CyberX's founding team built cloud security at AWS. This is a credibility signal that no amount of marketing spend can replicate. When selling to cloud-native organizations, 'built by the engineers who secured AWS' is a powerful narrative.
- **European regulatory expertise:** CyberX is natively architected for GDPR, NIS2, and DORA compliance. For European enterprises and any global company with EU operations, CyberX offers regulatory alignment that US-headquartered YSecurity must bolt on.
- **Multi-cloud independence:** CyberX is not funded by or aligned with any hyperscaler. YSecurity's lack of visible hyperscaler investment is comparable, but CyberX's AWS Ventures backing, combined with genuine multi-cloud depth, creates a 'trusted by AWS, works everywhere' positioning.
- **Runtime security depth:** CyberX Runtime Defense is a dedicated product with behavioral analysis and container runtime protection that goes deeper than YSecurity Runtime in live workload monitoring.
- **Capital efficiency:** CyberX has achieved ~45 customers on $85M in funding. YSecurity's customer count is not publicly disclosed despite $195M in capital. If CyberX's customer-to-funding ratio is superior, this efficiency narrative resonates with CISOs who value vendor sustainability.

Where YSecurity Wins vs. CyberX

- **More capital ($195M vs $85M):** The 2.3x funding gap translates directly into larger sales teams, more integrations (90+ vs 45+), faster product iteration, and broader analyst coverage. Capital is not everything, but in CNAPP, where enterprise sales cycles are long and integration requirements are deep, it matters.
- **Marquee enterprise logos:** JPMorgan, Microsoft, and Salesforce are reference customers that de-risk the evaluation for every subsequent CISO. CyberX's named customers (Barclays, Siemens, Unilever, NHS) are strong but carry less weight in the US market.
- **FedRAMP Moderate authorization:** CyberX lacks FedRAMP, which excludes it from the US federal market entirely. YSecurity's FedRAMP Moderate opens a large, sticky revenue segment that CyberX cannot access.
- **Three-product portfolio:** CNAPP, Runtime, and Shift-Left give YSecurity a broader surface for land-and-expand within enterprise accounts. CyberX's two-product portfolio covers cloud and runtime but lacks dedicated CI/CD pipeline security.
- **US headquarters and investor roster:** Summit Partners, Sequoia Capital, and Insight Partners are the most recognized names in enterprise SaaS investing. This investor roster signals 'winner' to US CISOs evaluating vendor longevity.

> **KEY CISO DECISION POINT**
>
> 'Where are your cloud workloads, and what regulations do you face?' For European enterprises under NIS2/DORA, CyberX's regulatory-native architecture is a genuine advantage. For US enterprises prioritizing breadth and FedRAMP, YSecurity currently leads. The battle is won account-by-account based on buyer geography and compliance requirements.

SECTION 06

Competitor Deep Dive: ZProtect [HIGH]

Founded	2019
Headquarters	Tel Aviv, Israel
Employees	340 (+8% YoY, stable growth)
Total Funding	$280,000,000
Last Round	Series D, $90M (June 2024)
Annual Revenue	~$85M (estimated)
Customers	500+ enterprises globally
Products	ZProtect Cloud, ZProtect Workload, ZProtect Container Security, ZProtect DSPM
Integrations	120+ including all major cloud providers and DevOps tools
Certifications	SOC 2 Type II, ISO 27001, HIPAA, FedRAMP High
Analyst Recognition	Gartner MQ Leader for Cloud Security, Forrester Wave Leader
Active Jobs	12
Momentum Score	61/100 (Accelerating)

The Established Incumbent

ZProtect is the mature, category-defining competitor that every CNAPP evaluation includes by default. With 500+ enterprise customers, Gartner MQ Leader status, Forrester Wave Leader recognition, ~$85M in estimated annual revenue, and FedRAMP High authorization, ZProtect represents the 'safe choice' that risk-averse CISOs default to when they do not have a compelling reason to choose otherwise. CyberX does not compete with ZProtect on breadth; it competes on depth, agility, and specialization.

ZProtect's four-product portfolio (Cloud, Workload, Container Security, DSPM) covers the broadest NIST CSF surface of any CNAPP vendor in this analysis. The DSPM product in particular addresses data security posture management, a rapidly growing sub-category that neither CyberX nor YSecurity have entered. At 340 employees with stable 8% YoY growth, ZProtect is in a mature scaling phase, optimizing existing revenue rather than aggressively acquiring new logos.

The strategic implication for CyberX: avoid direct feature-for-feature competition with ZProtect. Instead, compete on (1) multi-cloud discovery depth from AWS engineering pedigree, (2) European regulatory alignment, (3) deployment speed and agility vs. ZProtect's complex enterprise implementation cycles, and (4) pricing flexibility as a Series B company vs. a late-stage vendor with revenue targets.

Adjacent Market Analysis

ZProtect's expansion into DSPM (Data Security Posture Management) with a dedicated product signals a strategy to capture adjacent budget within existing accounts. This has two implications for CyberX:

- **Near-term:** ZProtect's DSPM product gives them a 'land and expand' vector that CyberX lacks. In competitive evaluations where both CNAPP and DSPM are on the CISO's roadmap, ZProtect wins on consolidation convenience.
- **Long-term:** If CyberX builds DSPM capabilities, it can compete on the same multi-product surface. However, building a fourth product before scaling the core two products is a resource allocation risk at Series B stage.
- **Strategic recommendation:** Partner with a DSPM vendor rather than build. This gives CyberX a competitive answer to ZProtect's breadth without diluting engineering focus on the core CNAPP and runtime security products.

SECTION 07

Competitor Deep Dive: MicroGuard [MEDIUM]

Founded	2022
Headquarters	Berlin, Germany
Employees	15 (stable)
Total Funding	Seed, $4,000,000
Products	MicroGuard Scanner (container security focused)
Active Jobs	2
Momentum Score	45/100 (Steady)

Boutique Container Security Specialist

MicroGuard is a Berlin-based seed-stage startup focused exclusively on container image scanning and vulnerability detection. At 15 employees with $4M in seed funding, MicroGuard is not a platform competitor. It competes in a single sub-segment (container security) where it delivers focused, developer-friendly tooling that some engineering teams prefer over the container scanning modules embedded in broader CNAPP platforms.

For CISOs, MicroGuard enters the conversation in two scenarios: (1) a DevOps team has already adopted MicroGuard Scanner and the CISO is deciding whether to keep it alongside a CNAPP platform, or (2) the organization needs only container scanning and does not require full CNAPP capabilities. In either case, CyberX should position MicroGuard as complementary (for the first scenario) or demonstrate that CyberX Runtime Defense delivers equivalent container scanning plus runtime protection, workload security, and CSPM that MicroGuard cannot provide.

The European connection is worth noting: both CyberX (London) and MicroGuard (Berlin) serve the EU market. If MicroGuard builds meaningful traction with EU-based container-native teams, they could become an acquisition target for a larger CNAPP vendor looking to strengthen EU presence. CyberX should monitor MicroGuard's customer growth and consider them as a potential acqui-hire if container security depth becomes a competitive gap.

SECTION 08

Threat Assessment Matrix

Each competitive threat is scored across five weighted dimensions that capture different aspects of competitive danger. Scores are based on verified data from the Mandos Cyber database, website analysis, and market signals. Platform vendors are assessed as a collective threat given their combined market power.

COMPETITOR	CATEGORY 25%	FUNDING 20%	GROWTH 20%	PRODUCT 15%	PLATFORM 20%	TOTAL	LEVEL
Platform Vendors	8	10	7	7	10	8.4	CRITICAL
YSecurity	9	8	9	8	5	7.9	HIGH
ZProtect	7	9	6	7	7	7.2	HIGH
MicroGuard	6	2	4	5	3	4.0	MEDIUM

Threat Assessment Matrix: Weighted Competitive Scores (Source: Mandos Cyber)

Scoring Methodology

CRITERION	WEIGHT	WHAT IT MEASURES
Category Overlap	25%	Same subcategory, same CISO budget line, same use case. Higher = more direct competition.
Funding Power	20%	Total capital raised, recent round size, investor quality. Higher = more GTM resources available.
Growth Velocity	20%	Employee growth, hiring velocity, ARR trajectory, web traffic trends. Higher = faster execution.
Product Overlap	15%	Direct feature competition, NIST coverage overlap, integration overlap. Higher = more head-to-head deals.
Platform Risk	20%	Likelihood of becoming embedded in a platform vendor's bundle. Higher = risk of commoditization.

Score Breakdown

COMPETITOR	CAT OVERLAP	FUNDING	GROWTH	PRODUCT	PLATFORM	WEIGHTED SCORE	THREAT LEVEL
Platform Vendors	8	10	7	7	10	8.4	CRITICAL

COMPETITOR	CAT OVERLAP	FUNDING	GROWTH	PRODUCT	PLATFORM	WEIGHTED SCORE	THREAT LEVEL
YSecurity	9	8	9	8	5	7.9	HIGH
ZProtect	7	9	6	7	7	7.2	HIGH
MicroGuard	6	2	4	5	3	4.0	MEDIUM

Threat Level Definitions

- **CRITICAL (8.0-10.0):** Existential threat requiring immediate strategic response. These competitors can win deals, attract talent, and consolidate market position within 6-12 months. Platform vendors collectively score CRITICAL because their bundled CNAPP capabilities remove CyberX from consideration entirely in single-cloud environments.
- **HIGH (6.0-7.9):** Significant threat requiring active monitoring and competitive positioning. YSecurity and ZProtect both score HIGH because they compete directly for the same enterprise budget line and can out-resource CyberX in sustained head-to-head competition.
- **MEDIUM (4.0-5.9):** Notable threat with limited current impact. MicroGuard competes in container security but lacks the product breadth, funding, or scale to threaten CyberX's core positioning.
- **LOW (1.0-3.9):** Minimal competitive threat. No current competitors in this analysis score LOW, though several niche open-source CNAPP tools exist in this tier.

SECTION 09

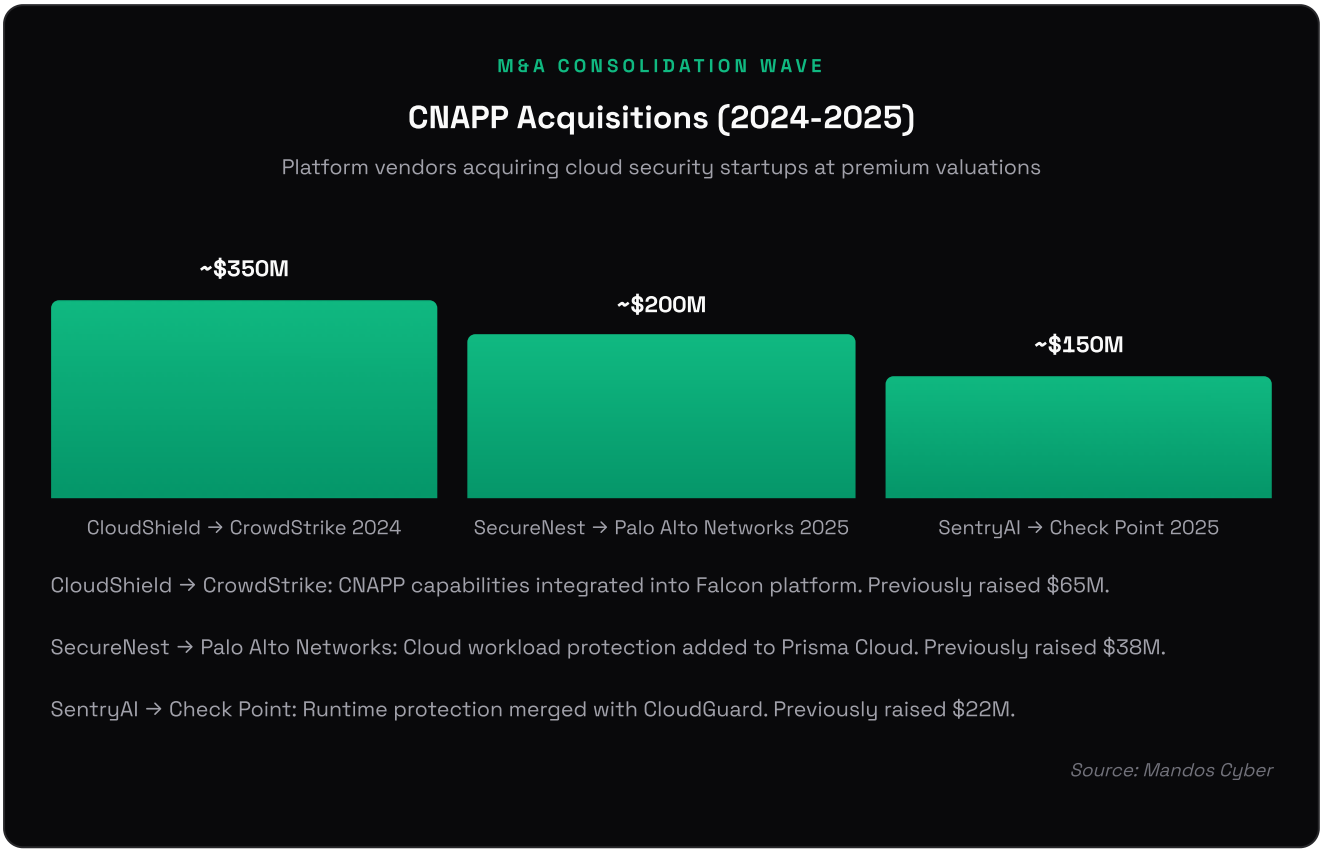
CNAPP Market Intelligence

Category Overview

Cloud-Native Application Protection Platform (CNAPP) is the fastest-growing security segment by funding velocity and vendor count. Mandos Cyber tracks 80+ products across CNAPP subcategories including CSPM, CWPP, Container Security, IaC Security, Cloud Workload Protection, and Cloud Infrastructure Entitlement Management (CIEM). Total funding deployed into the CNAPP category exceeds $4.2B, with major rounds continuing through 2025 (YSecurity's $120M Series C, ZProtect's $90M Series D). The category is driven by three forces: (1) multi-cloud adoption creating security complexity that legacy tools cannot address, (2) container and Kubernetes adoption requiring runtime-native security, and (3) regulatory pressure (NIS2, DORA, SOX, PCI DSS) mandating cloud security posture management.

Acquisition Consolidation Wave

The defining market event of 2024-2025 is the rapid acquisition of CNAPP startups by established platform vendors. Three acquisitions totaling approximately $700M+ have restructured the competitive landscape:



CNAPP M&A Consolidation: $700M+ in Acquisitions (2024-2025) (Source: Mandos Cyber)

~$700M	3	3	5-8x
TOTAL M&A VALUE	ACQUISITIONS	REMAINING INDEPENDENTS	AVG. PREMIUM

TARGET	ACQUIRER	EST. DEAL VALUE	PRIOR FUNDING	CATEGORY FOCUS
CloudShield	CrowdStrike	~$350M	$65M	CNAPP / Cloud Posture
SecureNest	Palo Alto Networks	~$200M	$38M	Cloud Workload Protection
SentryAI	Check Point	~$150M	$22M	Runtime Protection

Implications for CyberX

- **Validation signal:** Platform vendors paying $150M-$350M for CNAPP startups with $22M-$65M in prior funding validates the category and CyberX's market position. CloudShield's ~5.4x funding multiple suggests CyberX's $85M in funding could support a valuation floor of $200M+ in an M&A scenario.
- **Reduced independent competition:** Three competitors have been absorbed into platform bundles, narrowing the pure-play CNAPP field. However, unlike the AI security market where acquisitions removed most independents, the CNAPP category still has dozens of well-funded independent players.
- **Platform threat intensifies:** CrowdStrike (via CloudShield), Palo Alto (via SecureNest), and Check Point (via SentryAI) all now offer integrated CNAPP within their existing security platforms. CISOs who already use these platforms can add CNAPP without a separate procurement process.
- **Window is narrowing:** The pace of M&A suggests the market will consolidate further in 2026-2027. CyberX has 12-18 months to establish enough enterprise traction to either (a) remain independent as a category leader, or (b) command a premium acquisition price.

The Native Platform Threat

CISOs will increasingly ask: 'Why do I need a third-party CNAPP when my cloud provider or security platform offers it built-in?' This is the existential question for every independent CNAPP vendor, including CyberX.

- **AWS:** Security Hub, GuardDuty, Inspector, and Config provide native cloud security posture management for AWS environments. CyberX's founding team built some of these capabilities; the irony is that AWS's own tooling is now a primary competitor.
- **Microsoft:** Defender for Cloud provides CSPM, CWPP, and container security for Azure and multi-cloud environments. Microsoft's installed base and bundling strategy make Defender the default choice for Azure-primary organizations.
- **Google:** Security Command Center offers cloud security posture management for GCP. Weakest of the three hyperscaler offerings but improving rapidly with Mandiant integration.

- **CrowdStrike:** Falcon Cloud Security, now enhanced with CloudShield's CNAPP capabilities, integrates into the most widely deployed enterprise endpoint platform. CISOs already using Falcon face minimal friction adding cloud security.
- **Palo Alto Networks:** Prisma Cloud, now enhanced with SecureNest's workload protection, is the market-leading platform CNAPP. CISOs using Cortex XSIAM or Prisma Access can add CNAPP within the same vendor relationship.

CyberX's Counter-Narrative

The platform threat is real, but CyberX's counter-argument has substance: 'If you run workloads across two or more cloud providers, you need a vendor-independent CNAPP that provides consistent visibility and policy enforcement across all of them. AWS, Microsoft, and Google each optimize for their own cloud. CrowdStrike and Palo Alto optimize for their existing platform customers. CyberX optimizes for multi-cloud reality.'

This positioning is strongest when the buyer operates in two or more clouds (which Gartner estimates at 76% of enterprises by 2026). It is weakest when the buyer is single-cloud or already deeply invested in a platform vendor's security ecosystem.

Market Maturity Assessment

Based on all signals, the CNAPP market is in the GROWING to MATURING transition phase:

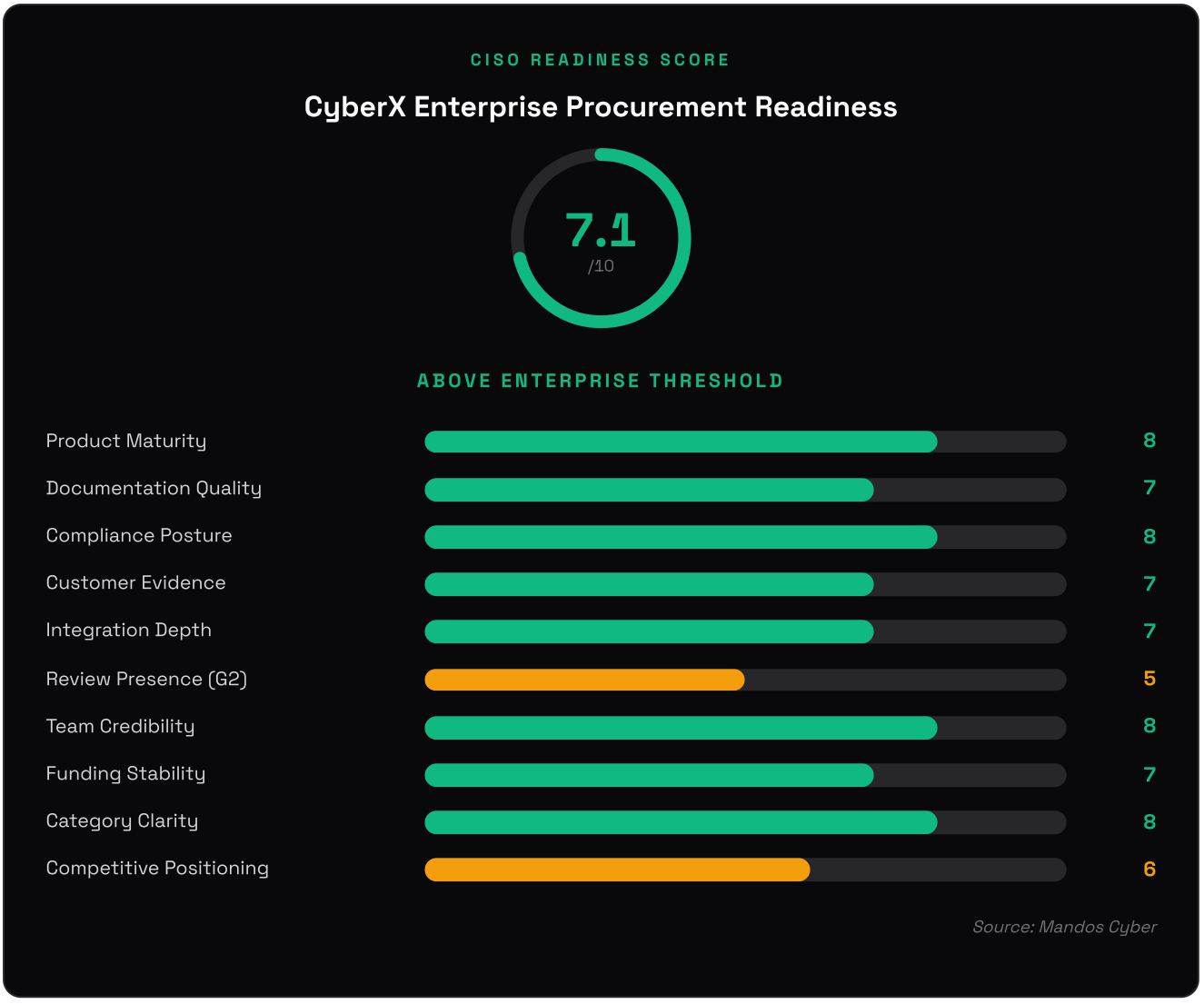
- **Growing signals:** New entrants still appearing weekly, VC funding at record levels ($4.2B+ deployed), category definitions still evolving (CNAPP vs CSPM vs CWPP vs CIEM boundaries remain fluid), Gartner and Forrester releasing dedicated category evaluations.
- **Maturing signals:** $700M+ in M&A consolidation, platform vendors embedding capabilities, pricing pressure from cloud-native free tiers, 80+ vendors creating buyer confusion and driving consolidation demand.

Estimated timeline: 18-24 months before the market structure solidifies into three tiers: (1) platform-embedded CNAPP (free/bundled), (2) enterprise-grade independent CNAPP (premium, multi-cloud), and (3) niche/point solutions. CyberX must establish itself firmly in tier 2 to survive.

SECTION 10

CISO Readiness Score

The CISO Readiness Score evaluates CyberX's preparedness for enterprise security procurement. Each criterion reflects what a CISO and their team verify during vendor evaluation, scored 1-10 based on verified evidence from website analysis, review platforms, database signals, and market context.



CyberX CISO Readiness Score: 7.1/10 (Source: Mandos Cyber)

#	CRITERION	SCORE	EVIDENCE	GAP
1	Product Maturity	8/10	Two products covering CNAPP + runtime, 45 customers, multi-cloud support, container scanning, IaC scanning	No dedicated CI/CD pipeline security product (YSecurity has Shift-Left)

#	CRITERION	SCORE	EVIDENCE	GAP
2	Documentation Quality	7/10	Technical docs available, architecture diagrams, integration guides on website	No public API reference or developer sandbox; ZProtect has comprehensive developer portal
3	Compliance Posture	8/10	SOC 2 Type II, ISO 27001, GDPR on dedicated /trust page; NIS2/DORA positioning	Missing HIPAA and FedRAMP (YSecurity has both); limits US healthcare and federal
4	Customer Evidence	7/10	Barclays, Siemens, Unilever, NHS logos visible; named references available	Logos without quantified case studies; no published ROI metrics or deployment timelines
5	Integration Depth	7/10	45+ integrations covering AWS, Azure, GCP, Splunk, CrowdStrike, Datadog, Jira	Half of YSecurity's 90+ and one-third of ZProtect's 120+; missing key DevOps tools
6	Review Presence	5/10	12 G2 reviews at 4.3/5; positive sentiment	Below the 30-review threshold where CISOs gain confidence; ZProtect has 200+ reviews
7	Team Credibility	8/10	Founded by former AWS security engineers; CTO from AWS; new CRO with enterprise track record	James Chen not widely known outside cloud security circles; needs more thought leadership
8	Funding Stability	7/10	$85M raised, Series B closed March 2025, strong investor mix including AWS Ventures	2.3x funding gap vs YSecurity ($195M); 3.3x gap vs ZProtect ($280M); Series C timing uncertain
9	Category Clarity	8/10	Clear CNAPP positioning; product names descriptive; multi-cloud narrative is coherent	Category boundaries with CSPM-only and CWPP-only vendors could be clearer for less technical buyers
10	Competitive Positioning	6/10	No comparison pages on website; no 'why CyberX vs alternatives' content visible	YSecurity and ZProtect both have competitive positioning; CyberX is ceding the narrative

7.1/10

OVERALL SCORE

CyberX scores solidly above the enterprise procurement threshold (6.0), meaning a CISO would proceed with evaluation rather than disqualifying during initial research. The score is anchored by strong product maturity (8), compliance posture (8), team credibility (8), and category clarity (8). Three fixable gaps prevent a score above 8.0:

1. **Competitive positioning (6/10):** No comparison pages, no 'why CyberX vs alternatives' content on the website. In the CNAPP category where CISOs evaluate 3-5 vendors minimum, the absence of competitive content forces CyberX's sales team to make the case in every meeting rather than letting the website pre-sell. Build dedicated 'CyberX vs YSecurity,' 'CyberX vs ZProtect,' and 'CyberX vs Platform CNAPP' pages immediately.
2. **G2 reviews (5/10):** 12 reviews at 4.3/5 is a solid foundation, but below the 30-review threshold where CISOs gain meaningful confidence. In CNAPP, where ZProtect has 200+ reviews and YSecurity is aggressively collecting reviews, 12 reviews positions CyberX as 'early' rather than 'proven.' Deploy a systematic review collection campaign targeting all 45 customers.
3. **Integration depth (7/10):** 45+ integrations cover the essential cloud providers and security tools, but the gap to YSecurity (90+) and ZProtect (120+) is visible to CISOs who compare integration pages. Prioritize CI/CD pipeline integrations (GitHub Actions, GitLab CI, Jenkins, CircleCI) and SIEM/SOAR platforms (Sentinel, Chronicle, Phantom) where gaps are most apparent.

CISO Buyer Check

Before requesting a demo, a CISO will: (1) Search Google for '[company] + cloud security', (2) Check G2 for peer reviews, (3) Search '[vendor] vs [alternative]', (4) Look for compliance badges and certifications, (5) Check LinkedIn for team size and hiring signals. Here is how CyberX performs:

CISO BUYER CHECK

Security Buyer Readiness Assessment

What CISOs verify before requesting a demo

✓ Enterprise Customer Logos — Fortune 500 logos: Barclays, Siemens, Unilever, NHS visible on site (STRONG)	✓ CISO-Level Testimonials — Named CISO quotes from Barclays, Siemens; VP Security from NHS (STRONG)
✓ Analyst Recognition — Gartner Cool Vendor 2025, Cyber Defense Magazine Top 10 (STRONG)	✓ Integration Ecosystem — 45+ integrations: AWS, Azure, GCP, Splunk, CrowdStrike, etc. (STRONG)
✓ Compliance Certifications — SOC 2 Type II, ISO 27001, GDPR displayed on /trust page (STRONG)	✓ Federal/Regulated Industry Credibility — NHS, financial services customers; UK Cyber Essentials Plus (STRONG)
~ Pricing Transparency — Enterprise pricing only; no self-serve tier visible (WEAK)	~ G2 / Peer Review Presence — 12 reviews on G2 (4.3/5); below category average of 50+ (WEAK)
✗ Competitive Comparison Pages — No "CyberX vs" pages found on website (MISSING)	~ Quantified Case Studies — Case studies exist but lack specific ROI metrics (WEAK)

Source: Mandos Cyber

CyberX CISO Buyer Check: Trust Signal Assessment (Source: Mandos Cyber)

6	3	1
STRONG	WEAK	MISSING

SECTION 11

GTM & Hiring Intelligence

CyberX GTM Signals

SIGNAL	CURRENT STATE	INTERPRETATION
Active Jobs	8 postings: 3 Enterprise AEs, 2 Senior Engineers, 1 Product Manager, 1 Solutions Architect, 1 Marketing Manager	Balanced growth across enterprise sales and product. Three Enterprise AE postings signal immediate GTM scaling under CRO David Park.
CRO Appointment	David Park (January 2026)	Enterprise sales acceleration signal. Appointed 10 months after Series B, suggesting product-first phase is complete and GTM scaling phase is beginning. Park's enterprise background (previously VP Sales at a cloud infrastructure company) signals intent to compete in enterprise accounts.
Customer Count	~45 across 3 segments	Solid for Series B; needs to reach 100+ for category leadership credibility and Series C positioning.
GTM Stage	Early enterprise scaling	Product-market fit established with named logos (Barclays, Siemens, NHS); now entering repeatable enterprise sales motion.
Marketing Manager Hire	1 open role	First dedicated marketing hire suggests shift from founder-led marketing to scalable demand generation. Late for Series B, but aligns with CRO-led GTM build.

YSecurity GTM Signals

SIGNAL	CURRENT STATE	INTERPRETATION
Active Jobs	15 postings (heavy enterprise sales + engineering)	Nearly double CyberX's 8 postings. Aggressive scaling signal consistent with deploying $120M Series C capital. Expect 15-20 enterprise AE hires in H1 2026.
Claimed ARR Growth	800% YoY	If accurate on even a modest base, this implies rapid enterprise adoption. Request absolute ARR numbers if possible; percentage growth on a small base can be misleading.
Named Customers	JPMorgan, Microsoft, Salesforce, Shopify	Tier-1 enterprise logos that function as a reference network. CyberX's Barclays and Siemens are comparable in Europe but less recognized in the US CNAPP market.

SIGNAL	CURRENT STATE	INTERPRETATION
Integration Count	90+ (vs CyberX's 45+)	2x integration advantage signals broader platform compatibility. CISOs evaluating CNAPP compare integration pages side by side.
FedRAMP Status	FedRAMP Moderate authorized	Opens US federal market entirely closed to CyberX. Federal CNAPP contracts are large, sticky, and defensible.

Competitive Hiring Analysis

The hiring signals reveal a critical dynamic: YSecurity is outpacing CyberX in GTM scaling velocity. Key observations:

- **Sales capacity gap:** YSecurity's 15 open roles include significantly more enterprise sales positions than CyberX's 3 AE postings. If YSecurity's sales team doubles by mid-2026 while CyberX adds 3 AEs, the pipeline generation gap will widen substantially.
- **Engineering investment:** CyberX's 2 Senior Engineer postings and 1 PM suggest continued product investment alongside GTM. This is the right balance at Series B; product depth is CyberX's competitive moat. However, YSecurity is also investing heavily in engineering, so the product advantage must be actively maintained.
- **Solutions Architect hire:** CyberX's open Solutions Architect role signals enterprise deal complexity increasing. SA-supported sales cycles are a sign of product maturity, as simpler products do not require dedicated SAs. This is a positive signal for CISOs evaluating technical depth.
- **Geographic strategy:** CyberX's London headquarters gives access to European enterprise talent. To compete in the US market (70%+ of CNAPP spend), CyberX will need US-based AEs. The 3 AE postings should prioritize US coverage.

SECTION 12

Strategic Recommendations & Battle Cards

30-Day Actions

1. **[Quick Win] Create competitive comparison pages vs YSecurity and ZProtect.** CISOs actively search '[vendor] vs [alternative]' during evaluation. Build dedicated pages: 'CyberX vs YSecurity' (emphasize AWS pedigree, European compliance, runtime depth, capital efficiency), 'CyberX vs ZProtect' (emphasize multi-cloud discovery, deployment speed, modern architecture, pricing flexibility), and 'CyberX vs Cloud-Native CNAPP' (address the platform bundling objection directly). Estimated effort: 2 weeks of content and design work. Impact: immediate improvement in competitive deal win rate.
2. **[Quick Win] Publish 3 quantified case studies (Barclays, Siemens, NHS).** Logo walls are table stakes. CISOs need measurable outcomes to justify procurement internally. Convert existing deployments to full case studies: Barclays ('Reduced cloud misconfiguration exposure by 87% across 3 clouds in 60 days'), Siemens ('Achieved NIS2 compliance for 12 manufacturing cloud environments in 45 days'), NHS ('Gained complete cloud asset visibility across 2,000+ workloads within 2 weeks'). Each case study must include Problem, Solution, Quantified Result, and a CISO or Security Director quote.
3. **[Quick Win] Launch 'European Cloud Security' positioning narrative.** CyberX's London headquarters and GDPR-native architecture are unique advantages in a market dominated by US and Israeli vendors. With NIS2 enforcement beginning in 2025 and DORA applying to financial services from January 2025, European enterprises face regulatory pressure that US CNAPP vendors address as an afterthought. Create a 'Built for European Cloud Security' campaign that positions CyberX as the CNAPP that understands EU regulatory requirements natively, not as a compliance module bolted onto a US product.
4. **[Fill-In] Get Verified on Mandos Cyber.** CyberX is listed with 2 tool entries but not verified. Verification provides: trust badge visible to 50,000+ monthly visitors (CISOs and security engineers), priority placement in the Cloud Security and CNAPP categories, and an SEO-optimized backlink from a high-authority cybersecurity domain. Visit mandos.io to complete verification.
5. **[Fill-In] Accelerate G2 review collection (12 is a good start, target 30+).** Deploy customer success to systematically request G2 reviews from all 45 customers. Provide a template email with direct link. Target: 30+ verified reviews in 90 days. The current 4.3/5 rating is strong; volume is the gap. In CNAPP, where ZProtect has 200+ reviews and YSecurity is actively collecting, 12 reviews positions CyberX as 'early stage' rather than 'proven enterprise.' Every CISO checks G2; low review count creates doubt that may be costing pipeline you never see.

90-Day Actions

1. **[Quick Win] Prepare Series C narrative and investor materials.** YSecurity's $195M in total funding and ZProtect's $280M create a capital perception gap. Whether CyberX raises Series C in 2026 or 2027, the narrative must be ready: capital efficiency ($85M to 45 customers vs YSecurity's $195M to undisclosed count), European market leadership, AWS founding pedigree, and a clear path to $50M ARR. Investor materials should quantify the European CNAPP TAM separately from the global TAM to demonstrate an addressable market where CyberX has structural advantages.

2. **[Major Project] Build regulated industries vertical (financial services + healthcare).** CyberX's strongest customer evidence (Barclays, NHS) is in regulated industries where compliance requirements create switching costs and long vendor relationships. Build a dedicated 'Financial Services Cloud Security' page and 'Healthcare Cloud Security' page with NIS2, DORA, PSD2, GDPR, and NHS DSPT compliance mapping. This vertical focus creates a defensible position that horizontal CNAPP vendors (YSecurity, ZProtect) cannot match without similar investment.
3. **[Major Project] Expand integration ecosystem from 45+ to 80+.** The integration gap to YSecurity (90+) and ZProtect (120+) is the most visible competitive weakness on a CISO's comparison spreadsheet. Prioritize: CI/CD tools (GitHub Actions, GitLab CI, Jenkins, CircleCI, ArgoCD), SIEM/SOAR (Microsoft Sentinel, Google Chronicle, Splunk SOAR, Palo Alto XSOAR), ticketing (ServiceNow, PagerDuty), and identity (Okta, Azure AD). Each integration should be documented with a setup guide and architecture diagram.
4. **[Quick Win] Pursue HIPAA certification.** CyberX has SOC 2 Type II and ISO 27001 but lacks HIPAA, which YSecurity and ZProtect both hold. For healthcare-sector CNAPP sales, HIPAA is a table-stakes requirement. Given CyberX's existing SOC 2 Type II compliance infrastructure, adding HIPAA is an incremental effort, not a greenfield build. Target completion within 90 days.

180-Day Actions

1. **[Major Project] Win European CNAPP category leadership.** No CNAPP vendor has established dominant European market position. US vendors (YSecurity) and Israeli vendors (ZProtect) serve European customers but do not lead with European-first messaging. CyberX should become the 'European CNAPP' through: (1) analyst briefings with Gartner and Forrester positioning European regulatory expertise, (2) speaking engagements at European security conferences (Infosecurity Europe, it-sa, Nordic IT Security), (3) European reference customers across 3+ countries, and (4) NIS2/DORA compliance content that positions CyberX as the authority. This is a 6-month sustained campaign, not a single initiative.
2. **[Major Project] Scale partner channel for European expansion.** Build a formal channel program with European MSSPs, system integrators, and cloud consulting firms. Partners who serve regulated European enterprises (Deloitte, Accenture, NCC Group, Capgemini) can drive pipeline that CyberX's direct sales team cannot reach at current scale. Target: 5-10 certified channel partners by end of 2026, contributing 20%+ of new pipeline.
3. **[Major Project] Prepare for platform era.** The acquisition wave signals eventual market consolidation into platform-embedded and independent tiers. CyberX should build enough enterprise value to either (a) remain independent as a European CNAPP category leader, or (b) command a premium acquisition price. Key targets: ARR above $30M, 100+ enterprise customers, Gartner MQ Visionary or higher placement. These metrics make CyberX attractive both as an independent company and as an acquisition target for platform vendors seeking European market access.

Battle Card: CyberX vs. YSecurity

For the sales team. Use when YSecurity appears in a competitive deal.

SECTION	CONTENT
Why They Win	1) $195M in funding signals stability and longevity to risk-averse CISOs. 2) JPMorgan, Microsoft, Salesforce logos are reference-quality enterprise customers. 3) FedRAMP Moderate opens the entire US federal market. 4) 90+ integrations cover more of the enterprise toolchain. 5) Forrester Wave Strong Performer provides analyst validation beyond Gartner. 6) Shift-Left product covers CI/CD pipeline security that CyberX does not.
Why They Lose	1) No AWS engineering pedigree; CyberX founders built cloud security at Amazon. Ask: 'Who built your cloud security engine, and how deep is their cloud-native experience?' 2) No European regulatory depth; NIS2, DORA, and GDPR are afterthoughts, not architecture decisions. 3) 800% ARR growth claim lacks absolute numbers; ask for actual ARR to assess the base. 4) Rapid 22% YoY headcount growth creates execution risk; fast hiring dilutes culture and product focus. 5) US-centric approach means European data sovereignty is a compliance add-on, not a core capability.
Land Mines They Plant	1) 'We have twice the integrations.' 2) 'Our Series C proves the market chose us.' 3) 'We have FedRAMP; do they?' 4) 'JPMorgan trusts us with their cloud security.' 5) 'We cover shift-left, cloud, and runtime; they only cover cloud and runtime.'
Counter Moves	1) 'Integration count is vanity. Ask which integrations are production-depth vs. checkbox. Our 45+ are deeply engineered by former AWS infrastructure engineers.' 2) 'Series C proves they need more capital to compete. We achieved comparable customer traction on 44% of their funding.' 3) 'FedRAMP matters for US federal. For European regulated industries under NIS2 and DORA, our compliance architecture is more relevant.' 4) 'Barclays trusts us with their cloud security. In European financial services, that reference carries equivalent weight.' 5) 'We chose to go deep rather than wide. Our runtime detection catches threats that surface-level shift-left scanning misses.'
Killer Questions for CISO	1) 'Do you operate in the EU or serve EU customers? If so, how does your CNAPP handle NIS2 and DORA compliance natively?' 2) 'How many cloud providers do you use? If more than one, do you want a CNAPP built by engineers from a single cloud, or one built by engineers who secured the world's largest cloud and then built for multi-cloud?' 3) 'What is your cloud security team's runtime detection requirement? Can your current evaluation demonstrate real-time workload behavioral analysis, not just posture scanning?'
When to Walk Away	If the CISO's primary need is US federal compliance (FedRAMP), CI/CD pipeline security (shift-left), or the evaluation heavily weights US-based enterprise references, YSecurity currently has structural advantages. Compete on runtime depth, European compliance, and multi-cloud engineering credibility. Do not compete on integration count or funding size.

Battle Card: CyberX vs. ZProtect

For the sales team. Use when ZProtect appears in a competitive evaluation.

SECTION	CONTENT
Why They Win	1) Gartner MQ Leader and Forrester Wave Leader provide the strongest analyst validation in CNAPP. 2) 500+ enterprise customers globally create an overwhelming reference network. 3) Four-product portfolio (Cloud, Workload, Container, DSPM) covers the broadest security surface. 4) FedRAMP High (not just Moderate) opens the most sensitive US federal workloads. 5) ~$85M in estimated ARR proves the business model at scale. 6) 120+ integrations are the deepest in the category.
Why They Lose	1) Seven years old (2019) with legacy architecture decisions; CyberX is cloud-native from day one. 2) Stable 8% YoY headcount growth signals maturity, not momentum. Buyers evaluating innovation may see ZProtect as the incumbent, not the innovator. 3) Complex enterprise implementation cycles (90+ day deployments reported) vs. CyberX's rapid deployment. 4) Premium pricing reflects market leader position; CyberX offers comparable core capabilities at Series B pricing. 5) Israeli HQ creates the same European data sovereignty concerns as US vendors for NIS2/DORA.
Land Mines They Plant	1) 'We are the Gartner Leader. Why risk an unproven vendor?' 2) 'We have 500+ customers; they have 45.' 3) 'We offer DSPM; they do not.' 4) 'Our FedRAMP High covers the most sensitive workloads.'
Counter Moves	1) 'Gartner Leaders are chosen for market position, not innovation. Ask ZProtect when their core architecture was last rebuilt. Our platform was designed for today's multi-cloud reality, not retrofitted.' 2) 'Customer count without retention data is incomplete. Ask ZProtect for net revenue retention. Our 45 customers include Barclays, Siemens, and the NHS, each actively expanding their deployment.' 3) 'DSPM is a valid need, but bundling it into your CNAPP creates vendor lock-in. We recommend best-of-breed DSPM alongside CyberX for optimal coverage.' 4) 'FedRAMP High matters for US federal. For the 76% of enterprises running multi-cloud outside federal, our multi-cloud depth is more relevant than a compliance certification for a market segment you may not serve.'
Killer Questions for CISO	1) 'How long did your last CNAPP deployment take? If ZProtect quotes 90+ days, ask why CyberX can deliver initial value in 2 weeks.' 2) 'When was ZProtect's core platform architecture designed? Cloud security requirements have changed dramatically since 2019. Kubernetes, serverless, and multi-cloud were not primary design constraints then.' 3) 'What is your total cost of ownership including professional services? Market leaders often bundle implementation costs that equal or exceed license fees.'
When to Walk Away	If the CISO requires DSPM as part of the CNAPP platform, needs FedRAMP High certification, or has a procurement policy requiring Gartner MQ Leaders only, ZProtect has structural advantages CyberX cannot overcome in the short term. Compete on deployment speed, multi-cloud depth, European compliance, and pricing. Do not compete on product breadth or analyst positioning.

Battle Card: CyberX vs. Platform Vendors

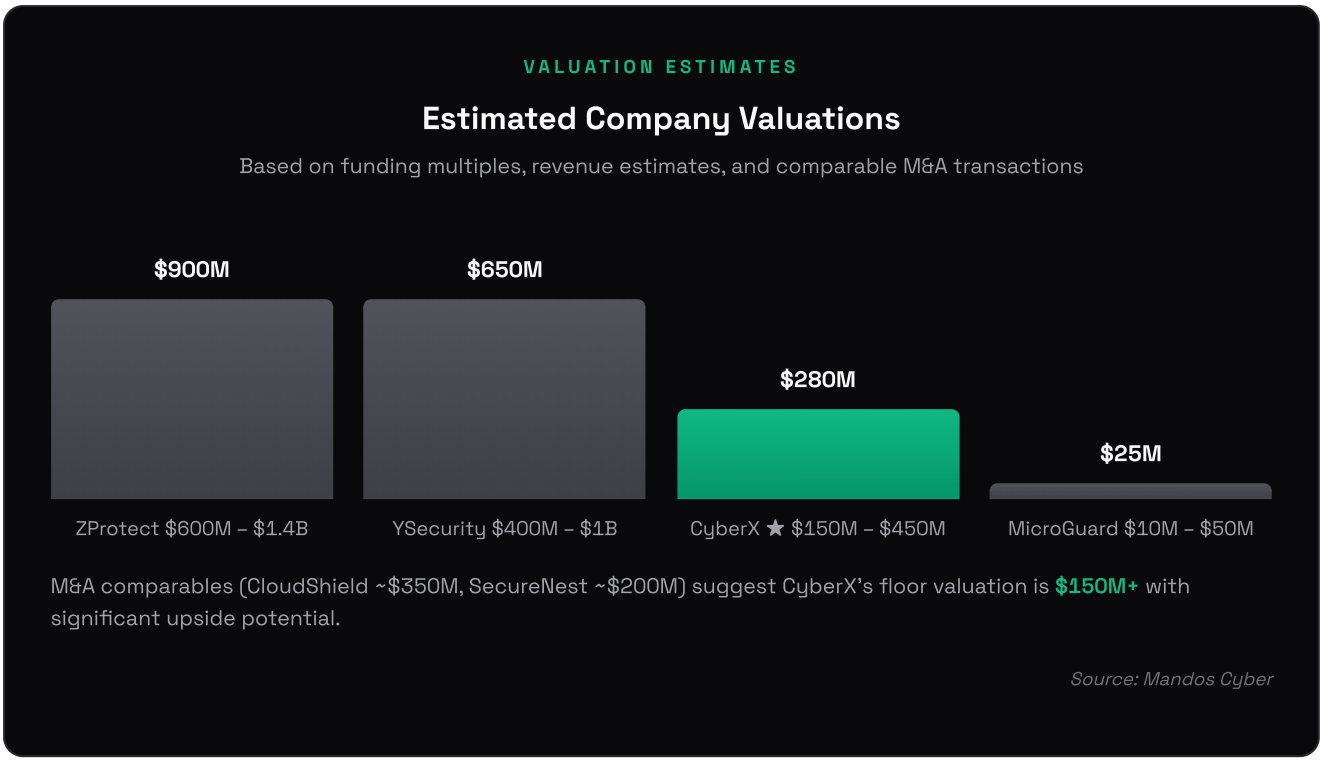
For the sales team. Use when the CISO asks 'Why not just use AWS/Microsoft/CrowdStrike/Palo Alto?'

SECTION	CONTENT
The 'Good Enough' Objection	'My cloud provider (or security platform) already has CNAPP capabilities. Why pay for another vendor?'
Counter Narrative	1) 'Platform CNAPP optimizes for their own cloud. CyberX optimizes for YOUR multi-cloud reality. If you run workloads on two or more providers, you need consistent visibility that no single-cloud tool can deliver.' 2) 'AWS Security Hub, Microsoft Defender for Cloud, and Google SCC each have blind spots in the other two clouds. CyberX was built by former AWS engineers specifically to eliminate these blind spots.' 3) 'CrowdStrike and Palo Alto acquired their CNAPP capabilities in the last 12 months. Integration is ongoing. Ask them how deeply CloudShield or SecureNest is integrated into their platform today vs. on their roadmap.' 4) 'Would you trust your endpoint security to a vendor that added it as a feature? The same logic applies to cloud security. Purpose-built defeats bolted-on when the stakes are this high.'
Proof Points	1) 'Barclays, Siemens, and the NHS chose a purpose-built multi-cloud CNAPP over platform features.' 2) 'Our founders built cloud security at AWS, then left because they knew a single-cloud approach could not solve the multi-cloud problem.' 3) 'We discovered 3x more cloud assets than AWS-native tooling in our Barclays deployment, including shadow cloud resources on Azure and GCP that AWS tools cannot see.'
Key Differentiators	1) Multi-cloud depth: consistent policy and visibility across AWS, Azure, and GCP from a single platform. 2) Independence: not tied to any hyperscaler's commercial incentives. 3) European data sovereignty: GDPR-native architecture, UK-headquartered, NIS2/DORA compliance built-in. 4) Runtime behavioral analysis: deeper than platform CNAPP modules that focus primarily on posture scanning.

SECTION 13

Valuation Estimates

Based on M&A comparable transactions, funding multiples, and revenue estimates, the following valuation ranges provide context for CyberX's strategic position and potential outcomes:



Estimated Valuation Ranges Based on Comparable Transactions and Funding Multiples (Source: Mandos Cyber)

M&A Comparable Analysis

Recent CNAPP acquisitions provide direct valuation benchmarks:

ACQUISITION	PRE-ACQUISITION FUNDING	ESTIMATED DEAL VALUE	IMPLIED MULTIPLE
CloudShield -> CrowdStrike	$65M	~$350M	~5.4x funding
SecureNest -> Palo Alto Networks	$38M	~$200M	~5.3x funding
SentryAI -> Check Point	$22M	~$150M	~6.8x funding

Applying comparable multiples to CyberX's $85M in funding suggests a valuation floor of $200M (conservative, ~2.4x funding, reflecting CyberX's earlier stage relative to CloudShield at acquisition) with a mid estimate of $425M (~5.0x, aligned with CloudShield and SecureNest multiples) and upside potential of $550M+ (~6.5x, aligned with SentryAI's premium multiple, achievable if CyberX demonstrates strong ARR growth before a transaction).

ZProtect's $280M in funding and Gartner MQ Leader status likely support a valuation exceeding $1B. YSecurity's $195M in funding at a post-money valuation likely between $600M-$800M (typical for $120M Series C at 3-5x post-money multiple). These valuations provide both upward benchmarks and acquisition-premium context for CyberX.

Strategic note: CyberX's European headquarters may command a geographic premium from acquirers seeking EU market access. Platform vendors (CrowdStrike, Palo Alto, Cisco) with limited European CNAPP presence would pay a premium for CyberX's regulatory expertise, UK/EU customer base, and NIS2/DORA compliance architecture. This 'European access premium' is not reflected in pure funding multiples but is a real factor in M&A negotiations.

SECTION 14

About & Next Steps

About This Report

This Mandos Benchmark Report was researched and written by Nikoloz Kokhreidze, Founder of Mandos Cyber and former enterprise security leader with 13 years of hands-on experience evaluating and procuring security solutions across banking, fintech, and FMCG.

Every insight, score, and recommendation reflects deliberate analysis, practitioner judgment, and pattern recognition built over years of sitting on the buying side of security decisions.

Intelligence Sources

Mandos Cyber serves as the primary data foundation, a cybersecurity market intelligence platform tracking 3,200+ companies and 8,500+ products. At the product level, the platform maintains deep intelligence across core features, integrations, deployment types, use cases, sector fit, NIST CSF 2.0 function coverage, pricing models, compliance posture, buyer classifications, and capability signals that reveal how a product actually positions in a real procurement decision, not just how it markets itself.

This structured data is combined with direct market observation across vendor positioning, customer evidence, go-to-market signals, funding history, headcount trends, momentum scores, and review sentiment patterns.

Methodology note: Some competitive signals are proprietary to Mandos Cyber and cannot be fully disclosed. What you see in this report is the output of that intelligence layer filtered through practitioner judgment.

Next Steps

- **Schedule a strategy call:** cal.com/nikolozk/30min
- **Monitor your competitors in real time:** mandos.io
- **List and verify your products:** mandos.io

Mandos Cyber | mandos.io