WINDSOR DRAKE

SIEM/SOAR Valuation Strategic Analysis & Market Intelligence Report : Q1 2026

JANUARY 2026

Executive Summary: The Great Bifurcation of 2026

Two distinct asset classes now define SIEM/SOAR valuations: AI-Native Platforms (premium multiples); Legacy Transitioners (compressed multiples).

WINDSOR DRAKE

AI-Native Platforms

20x+ EV/Revenue

Qualifiers: ≥20% growth, ≥30% FCF margins, Agentic AI.

Benchmark: **CrowdStrike ≈ 24.7x** (Jan 2026).

Legacy Transitioners

1.7x – 5.0x EV/Revenue

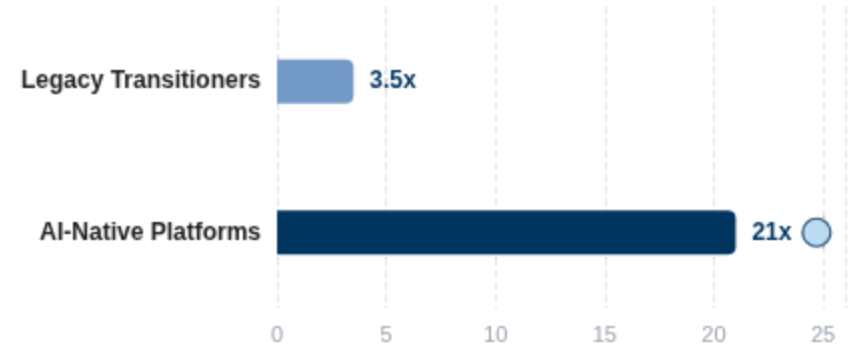
Headwinds: On-prem dependency, technical debt, retrofitted GenAI.

Represents mid-transition SIEM vendors.

- **Meritocratic capital allocation:** Premiums accrue to efficient, AI-native platforms; legacy tools face structural multiple compression.
- **$522B** forecast 2026 cybersecurity spend concentrates value in data-centric, agentic platforms.

Valuation Multiples Snapshot

EV/Revenue (indicative)



Note: CrowdStrike ~24.7x shown as benchmark within AI-Native cohort.

MARKET 2026

$522B

Global Cyber Spend

PLATFORM BENCHMARK

24.7x

CrowdStrike EV/Rev

REGIME SHIFT

Bifurcated

Merit > Momentum

Sources: Cybersecurity Ventures 2026 (market size); GuruFocus / Multiples.vc (CrowdStrike EV/Revenue); sector comps (legacy multiples).

Valuation Landscape Overview

Two distinct asset classes define 2026: AI-Native Platforms vs. Legacy Transitioners

WINDSOR DRAKE

AI-Native Platforms

20x+ EV/Revenue

GROWTH
≥ 20% YoY

FCF MARGIN
≥ 30%

Architecture
Agentic AI • Autonomous investigation & remediation • Data control plane

Benchmark
CrowdStrike trades at ~24.7x EV/Revenue (Jan 2026) reflecting platform breadth and efficiency.

Legacy Transitioners

1.7x–5.0x EV/Revenue

Profile

- Mid-transition to cloud architectures
- Technical debt; retrofitted GenAI features
- On-prem revenue durability questioned

Implication
Compressed multiples reflect execution risk and weaker unit economics.

Enterprise Value Concentration (Illustrative)

CONCENTRATION

Note: Visual illustrates premium value concentration among AI-native platforms consistent with 20x+ EV/Rev tiers; actual index composition varies by cohort.

Sources: Market observations Q1 2026; CrowdStrike public comps; sector trading ranges for legacy SIEM providers.

Macroeconomic Context & Capital Markets Outlook

Three forces shaping 2026 valuations: rates, AI capex, and M&A liquidity.

WINDSOR DRAKE

Equilibrium Management

Rates, discount factors, tax policy

Fed trajectory: Expected rate cuts into mid-2026 support long-duration software valuations. (MS 2026 Outlook)

Discount rate compression: Declining 10-year yields expand EV/Rev—allocation remains meritocratic.

$129B corporate tax relief: Through 2026–2027 bolsters FCF, reinforcing profitability focus.

Source: Morgan Stanley Investment Outlook 2026.

AI Capex Supercycle

Infrastructure and AI security demand

Hyperscaler spend: Microsoft ~**$50B** (2025 YTD) on AI data centers; Meta capex **$64–72B**.

AI spending: Forecast to exceed **$2T** in 2026—expanding attack surface requires AI Security Platforms.

Decoupling effect: Cyber platforms tied to the AI stack re-rate vs. broad software indices.

Sources: Aranca IT M&A (2025); Gartner AI spend (2026).

Return of M&A Animal Spirits

Credit availability and sponsor activity

Volume outlook: M&A projected **+20%** in 2026 after **+32%** recovery in 2025.

PE dry powder: Supports take-privates of sub-5x revenue cyber assets.

Valuation floor: Credit access sets a backstop for quality mid-caps in SIEM/SOAR.

Source: Morgan Stanley (2026); market observations.

RATES & VALUATIONS

Discount Rate ↓

Multiple expansion for efficient growth

AI INFRASTRUCTURE

$2T AI Spend

Security platforms benefit from capex

DEAL ENVIRONMENT

M&A +20%

Sponsors active; take-private window open

References: Morgan Stanley 2026 Outlook (8); Aranca IT M&A Q2-2025 (9); Gartner AI Spending (10); Investing.com/MS analysis on cybersecurity catalysts (12).

Market Sizing & Segmentation (2026)

Sizing for core Security Operations segments with growth and compliance drivers

WINDSOR DRAKE

Market Segment	2026 Size	Growth	Primary Growth Drivers
Global Cybersecurity	**$522B**	~15% CAGR	AI-driven threats, expanding attack surface, cross-functional budget shift (DevOps, IT, Legal).
SIEM / TDIR	**$11.3B**	14.5% CAGR	Compliance (SEC, GDPR), cloud migration, log retention and investigation scale.
Cloud Security	**N/A**	25.9% CAGR	Hybrid/multi-cloud complexity, shift-left security, Cloud-Native SIEM/CDR adoption.
Managed Services	**$42.1B** (est 2028)	15.0% CAGR	Global talent shortage; MSSP multi-tenancy; SOC outsourcing economics.
Data Privacy / Security	**$10.3B** (est 2028)	14.0% CAGR	Regulatory pressure (GDPR, CCPA, NIS2); DSPM; AI data governance.

Sources: Cybersecurity Ventures (Global spend); Splunk/IDC (SIEM); Gartner/IDC (segment CAGRs).

COMPLIANCE CATALYSTS

SEC Rules

Incident disclosure, board oversight, tighter reporting → SIEM/TDIR uplift.

GDPR/CCPA

Data privacy mandates → logging, audit trails, DSPM demand.

NIS2 / DORA

Operational resilience in EU; stronger control/retention standards.

AI Governance

LLM/AI security posture, model auditability, data lineage.

BUDGET SHIFT

15%+

Spend outside CISO

CLOUD-NATIVE PREMIUM

25.9%

CAGR (Cloud Security)

Key Growth Vectors: Q1 2026

Cloud Security • Managed Security Services • Infrastructure Protection

WINDSOR DRAKE

Cloud Security

Cloud-Native SIEM positioning

Fastest Segment

25.9% CAGR

Gartner forecast (fastest among security segments)

- Shift to **Cloud Detection & Response** and cloud-native pipelines
- Buyer preference for unified **TDIR** over legacy SIEM

Implication: Premium multiple for AI-native, cloud-first analytics.

Managed Security Services

MSSP multi-tenancy

Talent Gap

+15.0% Growth

SOC outsourcing driven by scarce expertise

- **Multi-tenant** workflows and service automation increase retention
- Agentic AI augments Tier-1, lowering MSSP unit costs

Implication: Platforms with MSSP-first features command a service premium.

Infrastructure Protection

AI/LLM security focus

Platform Control

$51.2B • 13.1%

2026 spend and growth trajectory

- Hardening **AI pipelines** and model governance expands scope
- Controls shift toward **exposure management** and runtime defense

Implication: Data/control-plane ownership drives valuation resilience.

Sources: Gartner Security Forecast (14); IDC/Market sizing (14); Report synthesis. Windsor Drake palette.

Agentic SOAR Shift: From Static Playbooks to AI Agents

Contrasting Traditional SOAR versus Agentic AI SOC. Valuation signals: legacy multiple compression vs. scarcity premium for AI-native platforms.

WINDSOR DRAKE

Traditional SOAR (Playbooks)

Scripted workflows • Operator-driven

- Static playbooks and brittle integrations; limited ability to generalize to novel threats.
- Human-in-the-loop escalation; constrained automation beyond predefined steps.
- Retrofit of GenAI onto legacy codebases; rising maintenance and technical debt.
- Customer value framed as “tool” for analysts; limited OPEX reduction proof.

Valuation: Legacy Multiple Compression

Market perception: transitionary/legacy

VS

Agentic AI SOC (Multiagent)

Autonomous remediation • Data-centric

- Multiagent systems plan, act, and learn; autonomous investigation and response.
- Outcomes focus: reduced MTTR, lower false positives, measurable SOC OPEX savings.
- AI-native architecture leveraging a security data fabric; strong “data gravity” moat.
- Platform trajectory: converged TDIR (SIEM + SOAR + XDR + Identity) vs point tools.

Valuation: Scarcity Premium

Market perception: AI-native platform

Positioning Implications

- Rebrand from “SOAR playbooks” to “Agentic SOC” with ROI-first proof (OPEX reduction).
- Prioritize data ownership and control (lake/fabric) to sustain AI model efficacy.
- Converge to platform modules (TDIR) to align with vendor consolidation mandates.

Signals: Gartner Top Strategic Tech Trends 2026 (Multiagent Systems, AI Security Platforms) and SOAR evolution toward autonomous agents.

Tier 1 Platform Kings: CrowdStrike (CRWD)

24.7x EV/Revenue • Hyperscale efficiency • Platform breadth (EDR + Identity + SIEM)

WINDSOR DRAKE

CrowdStrike | Platform Summary

24.7x EV/Rev

MARKET CAP	REVENUE GROWTH	GROSS MARGIN
$121B	**22%**	**75%**
Jan 2026	YoY	LTM

RULE OF 40	RULE OF X	EV/REVENUE
30%	**82%**	**24.7x**
SaaS standard	Efficiency metric	Top decile

Why Tier 1 (Strategic Rationale)

- Platform consolidation: **EDR + Identity + SIEM/XDR** increases attach and durability.
- Data gravity via unified telemetry drives superior detection efficacy.
- Agentic AI trajectory and automation translate into OPEX savings for customers.
- Scale economics and FCF discipline justify premium multiple.

Platform Consolidation Stack

Platform

EDR	IDENTITY	SIEM/XDR
Endpoint telemetry	Unified identity signal	TDIR analytics

Strategic Takeaways

- Premium reserved for AI-native platforms with durable growth and margin.
- Category convergence (TDIR) and vendor consolidation are valuation tailwinds.
- Evidence of ROI (reduced MTTR, automation) strengthens multiple resilience.

REFERENCE Q1 2026

Sources: CrowdStrike public comps & filings; GuruFocus EV/Revenue; sector trading data (Jan 2026).

Note: Metrics presented for benchmarking purposes. Windsor Drake branding applied.

Public Valuations: Tier 2 Efficient Growers

Observability and Zero Trust leaders with premium EV/Revenue multiples.

WINDSOR DRAKE

Datadog

Ticker: DDOG • Observability → Cloud SIEM convergence

Efficient Grower

EV/REVENUE	MARKET CAP
14.5x	$46.9B

Thesis: Strong net expansion and product velocity; security telemetry adjacent to core observability unlocks Cloud SIEM attach.

Zscaler

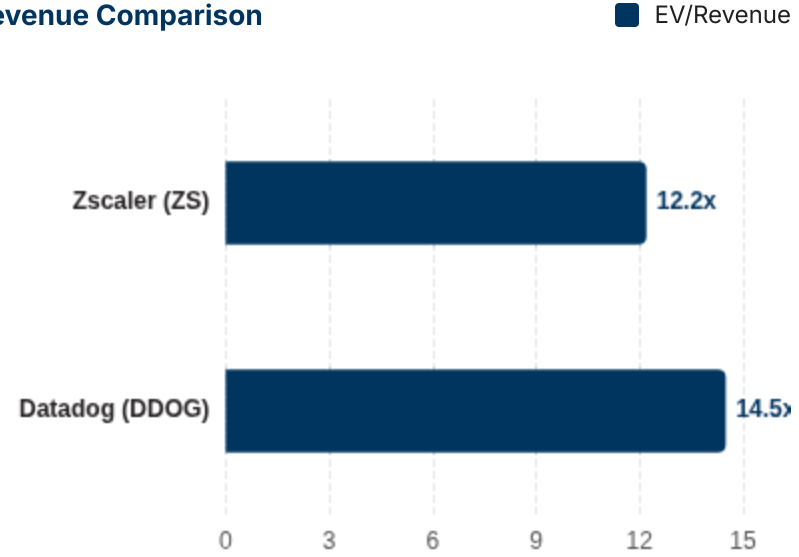
Ticker: ZS • Zero Trust Edge + Cloud Security

Efficient Grower

EV/REVENUE	EV/EBITDA	MARKET CAP
12.2x	77.8x	$34.6B

Rule of 80 profile: ~25% growth + ~55% FCF margin supports premium valuation vs. security median.

EV/Revenue Comparison



Data: Public comps (Jan 2026). Values rounded for illustration.

Banking Interpretation

Tier 2 “Efficient Growers” command 10x–15x EV/Revenue driven by durable growth and cash efficiency; clear security convergence narratives are key to sustaining premiums.

Sources: GuruFocus (DDOG, ZS); BVP/industry analyses. Figures reflect latest available as of Jan 2026.

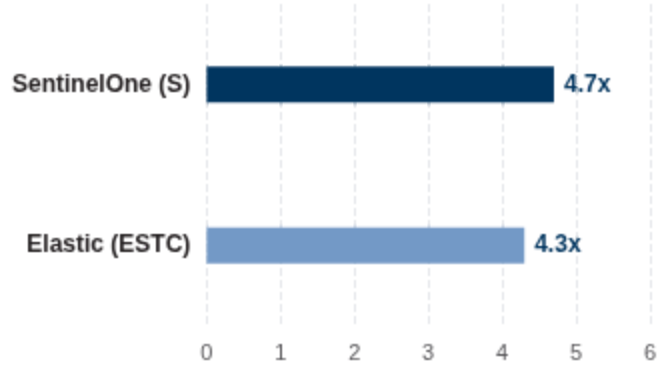
Public Valuations: Tier 3 Challengers (4x–8x EV/Revenue)

SentinelOne and Elastic operate with compressed multiples vs. platform leaders; execution toward profitable platform breadth is the catalyst.

WINDSOR DRAKE

EV/Revenue (LTM) Comparison

Tier 3



SENTINELONE
4.7x
EV/Revenue (LTM)

ELASTIC
4.3x
EV/Revenue (LTM)

INTERPRETATION

Discount reflects follower position vs. platform leaders (e.g., CRWD), transitional profitability, and perceived lag in unified data/AI control planes.

SentinelOne (S)

EV/Rev 4.7x | $5.3B Cap

EDR/XDR challenger progressing toward platform scale

GROWTH
20%
YoY Revenue

OP MARGIN
7%
Q3 FY26

POSITION
Challenger
Platform follower

Valuation Lens

Multiple reflects a **platform follower discount** vs. CRWD. Catalysts: AI-native SecOps modules, MSSP multi-tenancy, improving FCF trajectory.

Elastic (ESTC)

EV/Rev 4.3x | $7.6B Cap

Search-first analytics pivoting to Security & AI

GROWTH
16%
YoY Revenue

RULE OF 40
13%
Efficiency

PROFILE
Transition
Search AI pivot

Valuation Lens

Open-source legacy and lower profitability compress multiples. Upside from **Search AI** in security analytics and improved unit economics.

Sources: Multiples.vc; GuruFocus; company filings and commentary (Q1 2026). Metrics reflect latest publicly available data cited in report.

Public Valuations: Tier 4 Legacy Value

Rapid7 (RPD) as valuation floor for mid-cap SIEM vendors

WINDSOR DRAKE

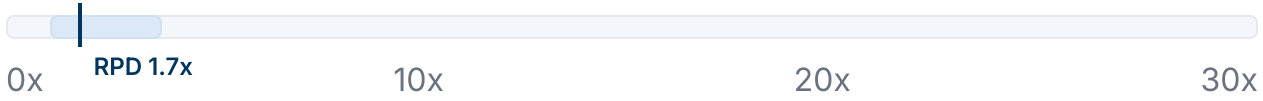
Rapid7

Ticker: **RPD**

LEGACY VALUE

EV/REVENUE	MARKET CAP	REVENUE GROWTH	RULE OF 40
1.7x	**$0.9B**	**~1%**	**-4%**
LTM multiple	As of Jan 2026	YoY	Efficiency

Valuation Band (EV/Revenue)



Note: Floor zone (1–3x) indicates distressed valuations typical of legacy transitioners; Tier 1 platforms trade 20x+.

Positioning: Distressed / PE Take-Private Candidate

Signal: Establishes floor for mid-cap SIEM valuations

Banking View & Implications

Legacy Transitioner: compressed multiples

- Valuation reflects investor skepticism on on-prem durability and cloud transition execution risk.
- Private equity playbook: take-private, cost discipline, product simplification, and MSSP channel optimization.
- Re-rating catalysts: sustained FCF improvement, NRR ≥120%, credible TDIR repositioning, and data-layer control.
- Sector context: defines a practical valuation floor for mid-cap SIEM vendors amid hyperscaler competition.

Sources: Rapid7 Valuation (4); SEG 2025 SaaS Index (26).

Public Company Valuation Table : January 2026

EV/Revenue, EV/EBITDA, P/E (Fwd), Market Cap, Revenue Growth, and Rule of 40/Rule of X

WINDSOR DRAKE

Company	Ticker	EV/Rev (LTM)	EV/EBITDA (LTM)	P/E (Fwd)	Market Cap ($B)	Rev Growth	Rule (40/X)
CrowdStrike	CRWD	**24.7x**	91.6x	126x	**$121**	22% YoY	**Rule of X 82%**
Datadog	DDOG	**14.5x**	N/A	N/A	N/A	N/A	High (Efficient)
Zscaler	ZS	**12.2x**	77.8x	N/A	$34.6	22% YoY	Rule of X ~80%
Fortinet	FTNT	**9.0x**	23.2x	32.6x	$56.0	14.8% YoY	High
SentinelOne	S	**4.7x**	Neg	Neg	$5.3	20% YoY	Rule of 40 ~ -10%
Elastic	ESTC	**4.3x**	35.2x	N/A	$7.6	16% YoY	Rule of 40 13%
Tenable	TENB	**2.8x**	N/A	N/A	$2.8	N/A	N/A
Rapid7	RPD	**1.7x**	9.3x	47.7x	$0.9	1% YoY	Rule of 40 -4%

Notes: Figures reflect latest available LTM metrics and market data as of Jan 2026. “Neg” denotes negative (not meaningful). “Rule of X” reflects growth-efficiency scoring used by investors.

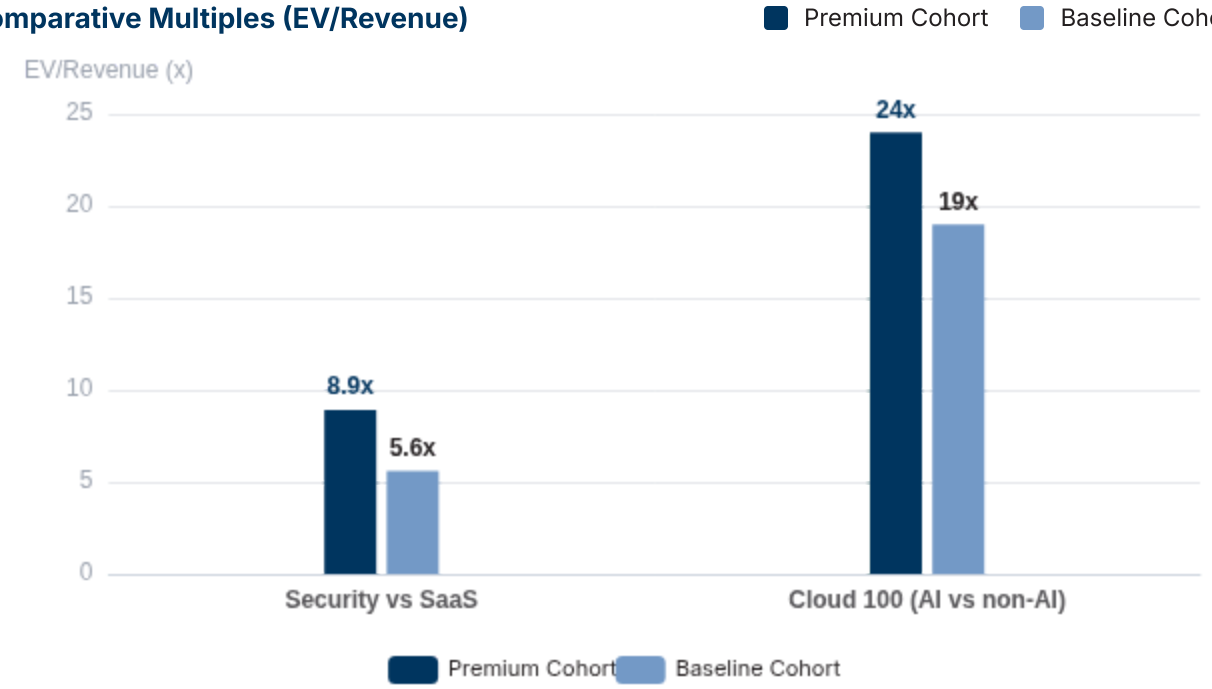
Source refs: 2, 4, 5, 17, 18, 22, 24, 25, 26 (GuruFocus, Multiples.vc, SEG SaaS)

Benchmark Analysis: Multiples & Retention Signals

Security vs. broader SaaS medians; retention premium; AI multiplier (SEG SaaS Index; Bessemer Cloud 100).

WINDSOR DRAKE

Comparative Multiples (EV/Revenue)



Notes: Security median reflects high-performing security companies (~8.9x) vs broader SaaS (~5.6x). AI-centric Cloud 100 companies trade at ~24x vs ~19x for non-AI peers.

RETENTION PREMIUM

11.7x EV/Rev

NRR ≥ 120% cohort commands a **109% premium** over peers.

Source: SEG SaaS Index.

SECURITY VS SAAS MEDIANS

Medians

8.9x Security

5.6x Broader SaaS

Implication: Security earns a structural premium due to mission-critical spend and consolidation tailwinds.

AI MULTIPLIER (CLOUD 100)

AI

24x AI-Centric

19x Non-AI

Source: Bessemer Cloud 100 Benchmarks.

Retention Drives Value

Sources: SEG 2025 Annual SaaS Report (retention premiums, medians); Bessemer Cloud 100 Benchmarks (AI multiplier). Figures are illustrative reference points for Q1 2026 valuation analysis.

PE Consolidation Wave: Arbitraging Public–Private Spread

Private equity playbook in SIEM/SOAR and adjacent analytics (2024–2026)

WINDSOR DRAKE

Darktrace → Thoma Bravo

CLOSED

AI-Native Threat Detection | Take-Private

VALUE	EV/REV	EBITDA
$5.3B	8.1x	34.2x

Premium reflects **AI-native positioning** and strong cash profile vs. legacy peers.

LogRhythm + Exabeam (Thoma Bravo)

CONSOLIDATION

SIEM + UEBA | Portfolio Merger

IMPLIED	TYPE	RATIONALE
~$2.5B+	Defensive	Scale

Combines on-prem install base with cloud UEBA to compete with **Microsoft Sentinel** economics.

Sumo Logic → Francisco Partners

RE-RATING

Cloud Analytics | Take-Private

VALUE	EV/REV	PREMIUM
$1.7B	5.6x	57%

Establishes a **valuation floor** for cloud-native analytics relative to public market troughs.

MARKET INTERPRETATION

PE is **arbitraging valuation dispersion** between public sentiment and intrinsic value, using scale and cost discipline.

Defensive consolidation is necessary for standalone SIEMs under hyperscaler pricing pressure.

Re-rating catalysts: durable FCF, NRR ≥120%, and credible TDIR repositioning with data-layer control.

References: Darktrace/Thoma Bravo (28,29); LogRhythm–Exabeam (6,30); Sumo Logic/Francisco Partners (31,32). Figures reflect cited deal reports.

Strategic Acquisitions: Data Layer & Platform Consolidation

Mastercard/Recorded Future and Palo Alto/QRadar SaaS signal data dominance and the sunset of legacy SIEM.

WINDSOR DRAKE

Mastercard → Recorded Future

Strategic

Threat Intelligence | Data Layer Thesis

DEAL VALUE
$2.65B
Announced

MULTIPLE
~6.5x
EV/Revenue (est)

PROFILE
Data
Intel ownership

Strategic Lens
Validates **Data Layer** as strategic control point; **non-security vertical** (FinTech) paying premium for proprietary threat intel.

Thesis: Data dominance • Intelligence network effects • Budget decoupling from CISO

Palo Alto Networks ← IBM QRadar SaaS

Asset Acq.

Asset Purchase | Cortex/XDR Consolidation

DEAL VALUE
$500M
Asset sale

RATIONALE
Customers
Migration

IMPLICATION
XDR
Platform scale

Strategic Lens
Signals the **sunset of legacy SIEM**; accelerates Cortex customer acquisition and **unified XDR** control plane.

Thesis: Customer migration • De-risked go-to-market • Vendor consolidation tailwind

Key Implications

Valuation & positioning signals for SIEM/SOAR.

- Data owners command higher multiples than log processors; **data gravity** drives strategic control.
- Asset purchases of legacy SaaS SIEM are primarily **customer acquisition** plays, not technology bets.
- **Vendor consolidation** (XDR + SIEM + SOAR) continues to compress point-solution valuations.
- Non-security buyers (FinTech) validate cyber as **critical infrastructure** with durable spend.

RECORDED FUTURE MULTIPLE
~6.5x Rev
Data premium vs SIEM

QRADAR SAAS OUTCOME
Legacy Exit
Accelerated migration

Sources: Mastercard/Recorded Future (7,33); Palo Alto/QRadar SaaS (34).

Major M&A Transactions (2024–2026) — SIEM/SOAR

Key consolidation events shaping valuation bands.

WINDSOR DRAKE

Target	Acquirer	Deal Value	Valuation Multiples	Deal Type	Strategic Rationale
Darktrace	Thoma Bravo	**$5.3B**	8.1x Rev / 34x EBITDA	Take-Private	AI-native asset; strong cash profile (28)
Recorded Future	Mastercard	**$2.65B**	~6.5x Rev (est)	Strategic	Threat intel data integration; data moat (7)
Sumo Logic	Francisco Partners	**$1.7B**	~5.6x Rev	Take-Private	Cloud SIEM consolidation; valuation floor (31)
QRadar SaaS	Palo Alto Networks	**$500M**	N/A (Asset)	Asset Acq.	Customer migration to Cortex; legacy SIEM exit (34)
LogRhythm + Exabeam	Thoma Bravo	**~$2.5B+ (imp.)**	Undisc.	Merger	Scale vs hyperscalers; UEBA + on-prem base (6)
Vectra AI	— (Funding)	**$1.2B val**	N/A	Funding	NDR/AI expansion signal (36)

Sources: 6, 7, 28, 31, 34, 36. Values reflect latest publicly reported or estimated terms; “imp.” denotes implied; “Undisc.” denotes undisclosed.

Strategic Lens: What This Signals

Consolidation and data-layer positioning drive premiums.

- PE establishing valuation floors for cloud SIEM and legacy transitioners; focus on operating leverage.
- Strategic buyers prioritize proprietary data assets and migration paths over standalone SIEM features.
- Hyperscaler pressure accelerates platform consolidation; agentic SOC capabilities command scarcity premiums.

Valuation Framework: Rule of 40 vs Rule of X

Evolution from simple growth-efficiency to a stricter capital-allocation standard in Q1 2026.

WINDSOR DRAKE

Rule of 40

Legacy standard for SaaS growth efficiency

Growth (%) + FCF Margin (%)

Threshold: ≥ 40% for premium consideration.

Top-quartile SaaS median: **40%+**; median performers: **~13%**.

Rule of X

Current investor lens for 2026

Growth (%) × Multiplier + FCF Margin (%)

Premium signal: High "X" scores justify double-digit EV/Revenue.

Efficiency-weighted; rewards profitable, durable growth.

CRWD BENCHMARK

Rule of X ~82%

Supports ~24x EV/Rev

PREMIUM THRESHOLD

≥ 40%

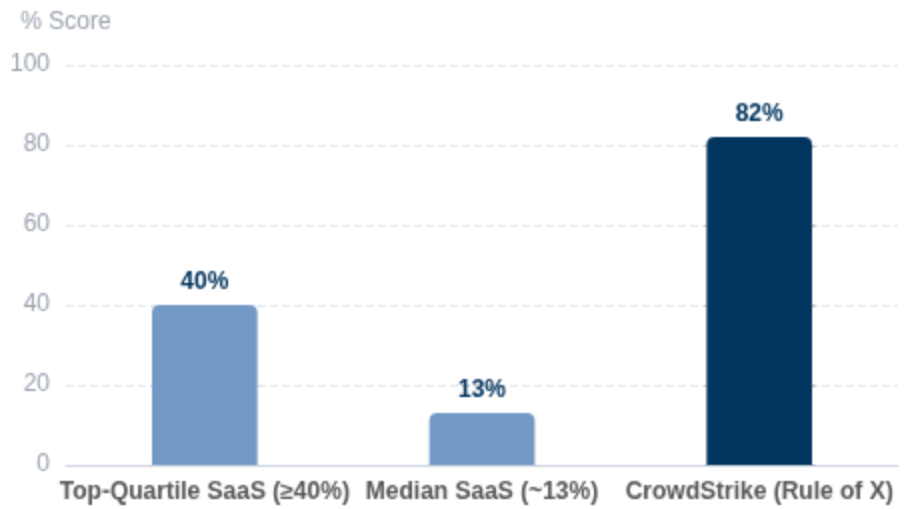
Top-quartile SaaS

EFFICIENCY TEST

$1 burn → >$1 ARR

Unit economics discipline

Growth-Efficiency Scores (Illustrative)



Note: CrowdStrike's Rule of X score (~82%) exemplifies elite efficiency; top-quartile median ≥40% vs. median ~13%.

Sources: Company filings; SEG SaaS benchmarks; internal synthesis.

AI-Native Architecture Premium

Valuation framework: AI-Washing (penalized) vs AI-Native (agentic automation) + Data Gravity thesis.

WINDSOR DRAKE

AI-Washing

ChatGPT bolted onto legacy UI

PENALIZED

- Superficial Q&A overlay; **no autonomous planning/execution**.
- Static playbooks and brittle integrations; limited impact on **SOC OPEX**.
- Data dependency on external stores; lacks **control of source data**.

VALUATION SIGNAL	PRODUCTIVITY	NARRATIVE
Compression	**Low**	**Feature**
Often 1–5x EV/Rev	No Tier-1 SOC repl.	“Pane of glass” add-on

AI-Native (Agentic AI)

Autonomous investigation & remediation

PREMIUM

- **Multiagent** systems with policies/guardrails; human-on-the-loop.
- Demonstrated **Tier-1 SOC analyst replacement** and measurable OPEX reduction.
- Owns/security-grades data pipeline for **closed-loop remediation**.

VALUATION SIGNAL	PRODUCTIVITY	NARRATIVE
Scarcity	**High**	**Platform**
Platforms 12–20x+ EV/Rev	Autonomous flows	TDIR / AI SOC fabric

Data Gravity Thesis

System of Record (Data Lake) valued higher than “pane of glass.”

Control the Data Layer

“Pane of Glass” (Viewer)

- Relies on external storage; **limited retention control**.
- Lower switching costs; weak data moat.

Relative valuation power (indicative)

System of Record (Security Data Lake)

- **Owns security data**, policy & retention; high attach/cross-sell.
- Higher switching costs; durable gross margin model.

Relative valuation power (indicative)

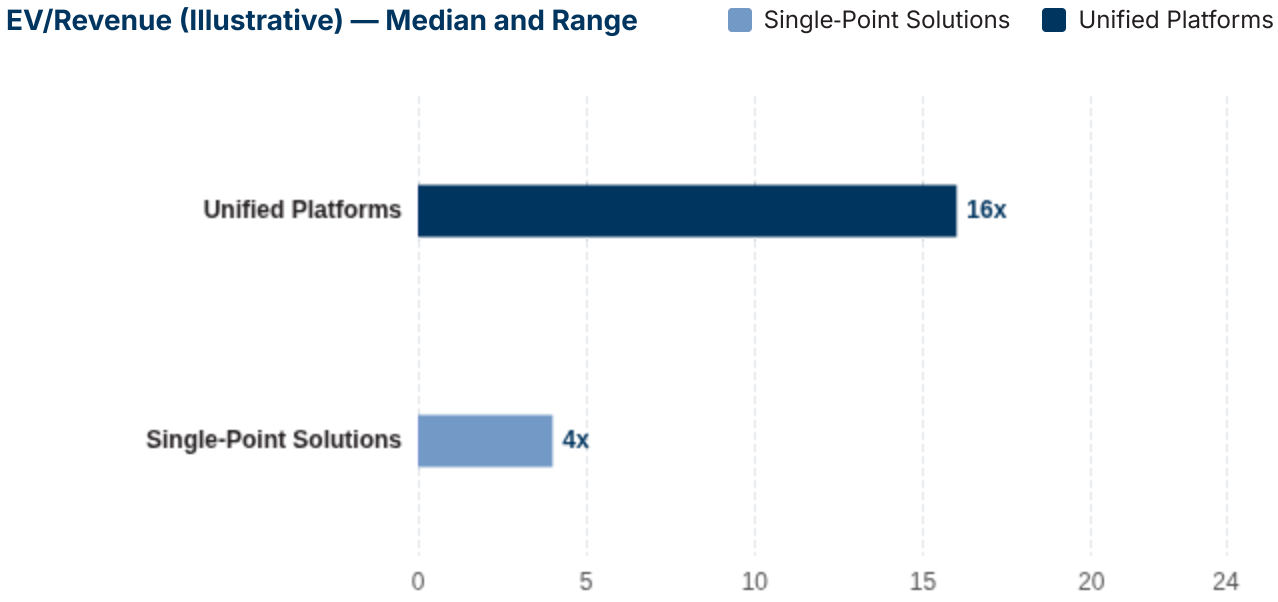
Investor takeaway: Platforms that **control the data plane** (not just visualize it) command structurally higher multiples.

Platform Consolidation Premium

Unified platforms (SIEM + SOAR + EDR + Identity) command premium EV/Revenue vs. single-point tools.

WINDSOR DRAKE

EV/Revenue (Illustrative) — Median and Range



SINGLE-POINT RANGE

~2x–6x

Compression as tools commoditize

UNIFIED PLATFORM RANGE

~12x–20x+

Premium for breadth, data gravity, AI

Consolidation Thesis

Platforms unify SIEM + SOAR + EDR + Identity to reduce vendor sprawl and unlock AI efficacy.

- Single-point tools face **valuation compression** (feature fatigue, limited control plane).
- **Unified platforms** command premium multiples via data gravity, cross-sell velocity, and agentic AI.
- **Vendor consolidation** is a structural tailwind: ~75% of enterprises are actively rationalizing security stacks.
- Budget share is shifting to platform leaders: **Palo Alto Networks (Cortex)** and **CrowdStrike (Falcon)** vs. standalone SIEMs.

CONSOLIDATION

~75%

Organizations pursuing vendor reduction

PLATFORM LEADERS

PANW • CRWD

Winning incremental wallet share

Notes: Ranges reflect banking synthesis across security software. Values indicative; actual multiples vary by growth, FCF, and AI-nativity.

Sources: Market synthesis; platform consolidation commentary; enterprise buyer surveys (Q1 2026).

Hyperscaler Competitive Threat

Microsoft Sentinel and Google Security Operations reshape SIEM economics; pure-plays must win on analytics efficacy.

WINDSOR DRAKE

Microsoft Sentinel

Hyperscaler

Commoditizing ingestion via enterprise bundles

- Bundled with **E5 licensing** and **Azure consumption**, pressuring log storage/ingest pricing.
- Shifts competition away from price of storage toward **analytics quality** and outcomes.

INGESTION PRICE PRESSURE

High (bundling + cloud credits)

Google Security Operations (Chronicle)

Hyperscaler

Planet-scale search; 2025 MQ **Leader**

- Leverages Google's infrastructure for **speed and scale** on historical security data.
- Improves long-horizon investigations; raises the bar for **query performance**.

SEARCH/SCALE ADVANTAGE

Leader-level capability

Strategic Implications

How pure-plays must reposition in the hyperscaler era.

- Compete on **analytics efficacy** (detection quality, time-to-signal, response automation) — not storage price.
- Adopt a **decoupled data layer** and open lake strategy; optimize for cost-to-ingest and retention control.
- Differentiate via **models, correlation, and SOC workflows**; partner with cloud marketplaces selectively.

WHERE TO WIN

Analytics

Quality > Quantity

AVOID COMPETING ON

Storage Price

Bundling undercuts

Sources: 2025 Gartner® Magic Quadrant™ for SIEM (Google Leader); Microsoft E5/Sentinel bundling; market synthesis.

Pure-Play Counter-Attack

Splunk (Cisco) pivots to Digital Resilience; Elastic advances “Open” Search AI + RAG to counter hyperscalers.

WINDSOR DRAKE

Splunk (Cisco)

Cisco

Market share leader; navigating innovator’s dilemma

- Pivoting to **Digital Resilience** and **Observability** to expand beyond pure security analytics.
- Leverages Cisco distribution; integrates security + ops telemetry for platform stickiness.
- **Innovator’s dilemma**: balancing legacy SIEM revenue with cloud-native modernization and AI.

STRATEGIC POSITION

Resilience Platform

Security + Observability convergence

RISK

Legacy Drag

On-prem ingestion economics

Elastic

Open

The “Open” alternative in SecOps

- Advancing **Search AI** and **RAG** for security contexts; faster triage with vector-augmented search.
- Undercuts hyperscalers on **flexibility** and **cost**; “open” ecosystem and portable data.
- Positions as **Cloud-SIEM alternative** with developer-first workflows and scalable search.

STRATEGIC POSITION

Search-Led SIEM

RAG + vector pipelines

EDGE

Open & Flexible

Lower TCO vs bundled SIEM

Strategic Analysis — Competitive Counter-Moves

Pure-Play Strategy

- Both aim to **differentiate vs hyperscalers** (Sentinel, Chronicle) on analytics efficacy, not storage price.
- **Stack convergence**: security + ops data; narrative shifts to resilience and open data fabrics.
- Valuation impact: execution on **cloud-native AI** and durability of gross margins are key to re-rating.

Context: Microsoft Sentinel bundling and Google Security Operations raise the bar on ingestion economics; pure-plays must win on analytic outcomes and openness.

Operational Metrics for Founders

Benchmarks required to achieve premium valuation in Q1 2026.

WINDSOR DRAKE

Growth Rate

High Growth requirement

> 30% YoY

Signals durable demand and category leadership.

Net Revenue Retention

Land-and-expand proof

120%+

Floor for premium valuation; proves platform expansion velocity.

Gross Margins

Operational efficiency

75%+

Indicates software leverage; not services-heavy.

Rule of 40

Balanced efficiency

> 40%

Ideal balance: **30% Growth + 10% FCF Margin**.

Investor lens: Companies meeting all four metrics qualify for double-digit EV/Revenue multiples in 2026, especially when paired with AI-native, platform positioning.

DESIGN SYSTEM

Palette: navy #00355f, medium #7399c6, light #acd4f1. Font: Inter.

Positioning for 2026: Founder Strategic Pivots

Strategic focus: reframe narrative, align to AI-era demand, and prove durable ROI.

WINDSOR DRAKE

Pivot 1

Reframe the category

Messaging

Drop “SIEM” → “TDIR” or “Security Data Fabric”

- Retire legacy baggage: high cost, low value perceptions tied to SIEM.
- Position around Threat Detection, Investigation & Response (TDIR) and a modern data fabric.
- Lead with control of the data plane, not just a “pane of glass.”

Outcome: Improved win rates vs. legacy and clearer enterprise value narrative.

Pivot 2

Own the next control plane

Product

Focus on Non-Human Identities (NHI)

- AI agents and service accounts are exploding —massive greenfield opportunity.
- Unify identity for human + machine; enforce least privilege across pipelines.
- Integrate with CI/CD, secrets, API gateways to secure automated workflows.

Outcome: Differentiation vs. legacy SIEM; identity-anchored AI SOC roadmap.

Pivot 3

Prove economics

Go-to-Market

Prove the AI Efficiency Dividend

- Demonstrate measurable SOC OPEX reduction (ticket time, FTE hours, false positives).
- Adopt ROI-first sales motion aligned to 2026 budget scrutiny.
- Publish before/after benchmarks and customer payback periods.

Outcome: Premium multiple eligibility; proof of durable, profitable growth.

Strategic Takeaway

Reposition around TDIR/Data Fabric, anchor in NHI control, and quantify AI-driven cost savings to qualify for double-digit EV/Revenue valuation bands.

Palette: Windsor Drake (navy #00355f)

AI Capex Supercycle: Impact on Cybersecurity

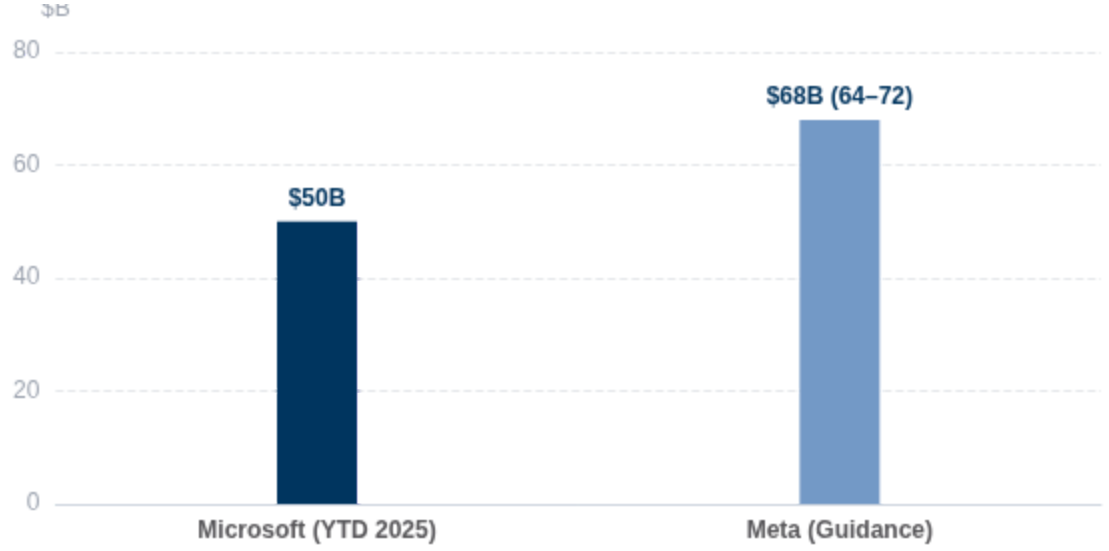
Q1 2026

Big Tech capex and $2T AI spending expand the attack surface; AI Security Platforms become essential defenders.

WINDSOR DRAKE

AI Infrastructure Capex (Illustrative, $B)

Microsoft YTD 2025; Meta 2026 guidance range



MICROSOFT

$50B

AI data centers (YTD 2025)

META

$64–72B

Capex guidance (2026)

Strategic Impact: Why It Matters

Capex → Attack Surface → Security Platform Premium

- Gartner projects **$2T AI spending in 2026**; security must scale with AI infrastructure growth.
- Creates a **massive new attack surface** across models, data pipelines, and inference endpoints.
- **AI Security Platforms** (agentic, data-centric) emerge as **essential defenders** for hyperscale environments.
- Category decoupling: cybersecurity positioned with **long-duration growth** alongside AI enablers.

AI SPEND 2026 (GARTNER)

$2 Trillion

Macro catalyst for security platform demand

Notes: Bars indicative for scale; Meta shows midpoint with annotated range.

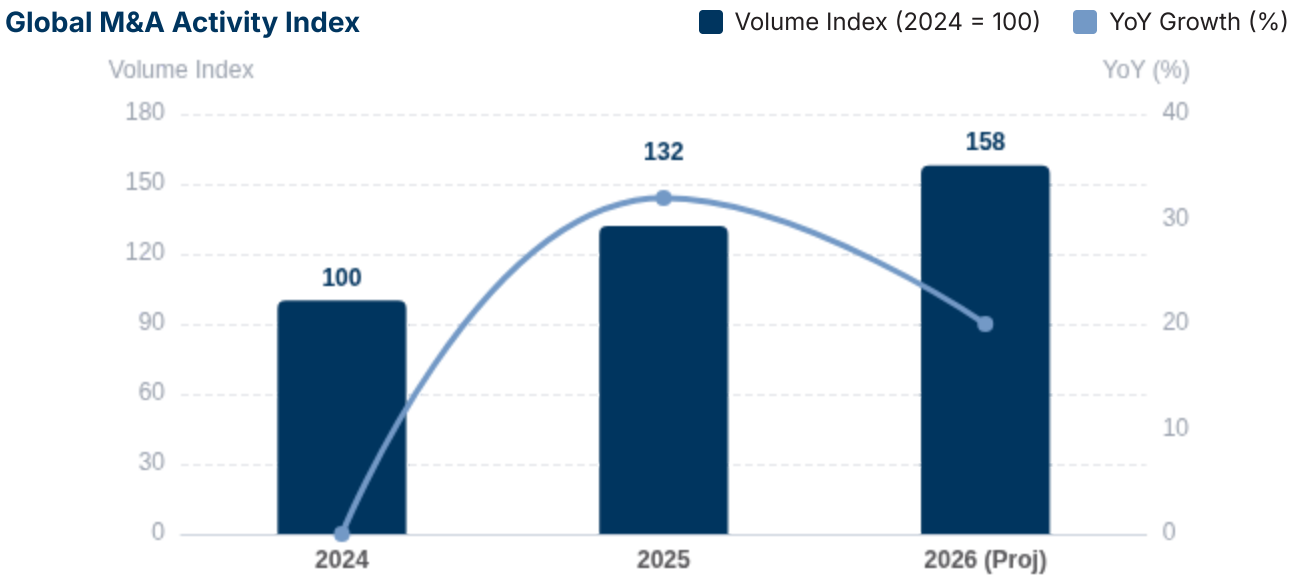
Sources: Aranca IT M&A (Big Tech capex); Gartner AI spending; Morgan Stanley thematic insights.

M&A Volume Growth Projection (2025 → 2026)

Credit markets, PE dry powder, and take-private dynamics set valuation floors for cyber.

WINDSOR DRAKE

Global M&A Activity Index



2025 RECOVERY
+32%
Versus 2024

2026 PROJECTION
+20%
Volume growth

PE DRY POWDER
>$1T
Leverage capacity

TAKE-PRIVATE FLOOR
<5x EV/Rev
Valuation arbitrage

Credit Markets: Banking Signals

What enables a busier M&A calendar in 2026.

- Resurgence in deal-making signaled by improving credit availability; **+20% M&A volume** projected for 2026 after a **+32% recovery** in 2025.
- **Investment-grade spreads** widen on heavy AI capex issuance; **high-yield remains insulated**, preserving sponsor financing channels.
- **Ample PE dry powder** supports leveraged buyouts and add-ons across cyber infrastructure categories.
- **Take-private dynamics** set a valuation floor for mid-cap cyber assets trading **<5x EV/Revenue** (public-to-private arbitrage).

Sources: Morgan Stanley 2026 Outlook; Aranca 2025; internal synthesis. Windsor Drake palette.

Conclusion: Q1 2026 SIEM/SOAR Valuation

Robust market, strictly meritocratic. Efficient, AI-driven scale era begins.

Q1 2026

WINDSOR DRAKE

Meritocratic Market — The Great Bifurcation

$522B rising tide is not lifting all boats equally

- AI-Native Platforms earn a scarcity premium with **20x+ EV/Revenue** multiples when paired with hyperscale efficiency.
- Legacy Tools in transition face **commoditization (2–4x EV/Revenue)** amid cloud migrations and technical debt.
- Path to value: deliver **Rule of 40+**, adopt **Agentic AI architectures**, and position as an **automated platform for business resilience** (not merely an analyst tool).
- The **growth-at-all-costs era is closed**; investors reward efficient, AI-driven scale with durable unit economics.

Rule of 40+ | Agentic AI | Resilience Platform | Efficiency First

Valuation Split (Illustrative)

MARKET CONTEXT

$522B

Global cybersecurity spend (2026 est.)

INVESTOR LENS

Efficiency > Growth

Premium linked to cash-flow quality

Note: Bars are illustrative for emphasis; actual multiples vary by growth efficiency, AI nativity, and platform breadth.

Summary: Investors bifurcate SIEM/SOAR into AI-native platforms vs. legacy transitioners. To re-rate, prove Rule of 40+, agentic automation, and business resilience outcomes.

Key Takeaways

Investment lens for Q1 2026 SIEM/SOAR valuations.

WINDSOR DRAKE

Valuation Bifurcation is Structural

AI-native vs. legacy gap is widening

- Not cyclical: quality premium persists as investors reward efficiency and AI-nativity.
- **Spread endures:** CrowdStrike **24.7x** EV/Rev vs Rapid7 **1.7x**.
- Legacy transitioners remain compressed (1.7x–5x) absent re-platforming.

Implication: Asset class split is durable; underwriting must reflect structural rerating.

The Agentic AI Moat

Autonomous SOC platforms command premium

- Multiagent systems plan and execute remediation—replacing Tier-1 analyst workload.
- Static playbooks are effectively **obsolete**; agentic AI signals durable advantage.
- Premium multiples accrue to **AI-native architectures**, not AI-wrappers.

Implication: Demonstrable AI OPEX reduction strengthens the valuation case.

Platform Wins Budget Share

Consolidation favors unified control planes

- **~75%** of buyers pursue vendor consolidation in 2026.
- Unified **SIEM + SOAR + EDR + Identity** platforms outcompete point solutions.
- Point solutions face **multiple compression** absent platform attach.

Implication: Platform narrative and attach rate metrics drive re-rating potential.

Palette: navy #00355f, medium #7399c6, light #acd4f1. Font: Inter.

Sources & References

Comprehensive bibliography of valuation metrics, market intelligence, and transaction data underpinning the Q1 2026 analysis.

WINDSOR DRAKE

Public Company Valuation Data

GuruFocus Metrics (LTM/Fwd)

- CrowdStrike (CRWD): EV/Revenue Multiples
- Datadog (DDOG): EV/Revenue Analysis
- Zscaler (ZS): EV/Revenue Trends
- Fortinet (FTNT): EV/EBITDA Valuation
- Tenable (TENB): EV/Revenue & Growth
- SentinelOne (S): Enterprise Value
- Elastic (ESTC): Valuation Ratios

Multiples.vc (Public Comps)

CrowdStrike • Zscaler • Elastic • SentinelOne • Rapid7
(Comparative Peer Group Analysis)

Market Research & Trends

- Cybersecurity Ventures: 2026 Market Report
- Gartner: Top Strategic Technology Trends 2026
- SEG: Annual SaaS Report (2025 Edition)
- Bessemer VP: Cloud 100 Benchmarks (2025)

Key M&A Transactions

Darktrace → Thoma Bravo
$5.3B Take-Private (Source: SecurityWeek)

LogRhythm + Exabeam
Merger of Equals (Source: Thoma Bravo Press)

Mastercard → Recorded Future
$2.65B Acquisition (Source: Channel Futures)

Sumo Logic → Francisco Partners
$1.7B Take-Private (Source: PE Hub)

Palo Alto Networks → IBM QRadar
$500M SaaS Asset Acquisition (Source: CRN)

Investment Banking & Capital Markets

- Morgan Stanley: 2026 Investment Outlook
- Aranca: IT M&A Deal Trends (Q2 2025)
- PitchBook: Cyber Deal Flow Analysis

Industry Commentary & Trade Pubs

- Splunk: "SIEM Explained" (Core Concepts)
- Radiant Security: "SOAR in 2026" (Agentic Shift)
- SentinelOne: SIEM Vendors Landscape (2025)
- Forrester: 2026 Cybersecurity Predictions
- CRN: SIEM Consolidation Coverage

Note: Financial figures reflect LTM or most recent quarter filings as of Jan 2026. This appendix supports valuation, market sizing, and transaction analyses presented in the main report.