CrowdStrike Investment Memo

Company Overview: CrowdStrike Holdings, Inc. (NASDAQ: CRWD) is a leading global cybersecurity company that delivers cloud-native endpoint protection. The Falcon platform is CrowdStrike's flagship product and comprises several modules, including endpoint detection, threat intelligence, vulnerability management, and proactive security services, allowing for a flexible and tailored suite of product offerings based on customer needs. CrowdStrike generates approximately 95% of its revenue from subscriptions.

Since its IPO in 2019, CrowdStrike has grown significantly, driven by the rising demand for cybersecurity solutions amid increasing threats and regulatory pressures. 'Platformization' has also driven demand for CrowdStrike, as enterprises are increasingly turning to large platforms with broad offerings for their cybersecurity needs. But on July 19th, 2024, CrowdStrike's outage caused the stock price to drop dramatically, from a high of $398 per share to a low of around $217 per share. Since then, the stock has begun to rebound and currently trades at $355 per share. In the past few months, the market has become less fearful of the potential churn of existing customers following the outage. However, there remain debates concerning the impact of the outage on the acquisition of new customers, potential FCF margin compression in the short term, and whether nnARR will decrease in the short term.

1) Superior Technology & Operational Excellence as Competitive Moat

CrowdStrike has established itself as a leader in the endpoint detection and response (EDR) market, driven by its best-in-class Falcon platform. Falcon leverages AI and machine learning to provide unparalleled threat detection, endpoint protection, and proactive security measures. CrowdStrike is currently ranked first in the Gartner Magic Quadrant 2024 Report for EDR platforms, a leading technological research report that enterprises heavily consider when choosing what technologies to implement. Its OverWatch team, which actively hunts for threats in customer environments, differentiates the company from competitors like SentinelOne, Microsoft Defender, and Palo Alto Networks.

Active Threat Hunting: The OverWatch team goes beyond basic monitoring; instead, it proactively searches for threats, significantly reducing the response time in the case of a breach. Industry professionals with 20+ years of experience note CrowdStrike's unmatched detection rate across various Red Team exercises and bake-offs. Alerts from OverWatch are treated with utmost seriousness, indicating its high fidelity and precision in detecting potential breaches. This is a key differentiator in a market where response speed can make the difference between preventing a breach and suffering severe damage and losing sensitive information and data.

Ease of Deployment and Integration: Falcon is noted for its user-friendly deployment and scalability, especially compared to competitors like SentinelOne. The simplicity of integrating CrowdStrike into existing infrastructure reduces onboarding time and associated costs, which is crucial for enterprises seeking quick implementation of EDR protection services. This is a

significant competitive advantage, especially for Managed Detection and Response (MDR) partners who sit between CrowdStrike and end customers.
Customer Stickiness & High Switching Costs: Once customers are onboarded, the combined power of Falcon and the OverWatch team's capabilities creates high switching costs. Given the complexity of migrating cybersecurity solutions and the certifications tied to CrowdStrike's ecosystem, customers are reluctant to move to alternative providers. Even after CrowdStrike's outage in July 2024, an overwhelming percentage of current CrowdStrike customers expressed that they planned to remain with CrowdStrike. This stickiness translates to a strong subscription renewal rate (95% of revenue) and low churn.
Key Bet: We believe that CrowdStrike's superior technology will lead to increased customer growth (~100 bps additional growth than Street) and ability to continue raising price (~8-9% per year) after the discounts from the incident subside. We underwrite a ~26% revenue growth till 2029 vs a Street consensus at ~23%.

2) Misunderstood Gross Margin Expansion Potential Due to Cloud Efficiency
CrowdStrike's gross margin improvement potential is often underestimated due to a lack of focus on its aggressive cloud cost optimization strategy. With cloud hosting costs accounting for over 50% of its cost of goods sold (COGS), the company's partnerships and investments in optimizing cloud infrastructure are poised to drive substantial efficiencies and profitability gains.
Cloud Cost Optimization Initiatives: CrowdStrike recently partnered with Google Cloud to power Mandiant's Incident Response and Managed Detection and Response services. This partnership with Google Cloud has the potential to reduce cloud hosting costs by leveraging Google's infrastructure efficiencies, with Google Cloud generally being a more affordable product than AWS. Additionally, the company's investments in AI to optimize data processing and storage will reduce cloud expenses.
AWS vs Google Cloud: On average, Google Cloud is ~10%-20% cheaper than AWS for comparable services, particularly in storage and compute-intensive tasks like threat detection and endpoint monitoring. Example:

- **Compute Costs:** Google Cloud's per-second billing model and sustained-use discounts make it more cost-effective for workloads running consistently, which is common for CrowdStrike's Falcon platform.
- **Storage Costs:** Google Cloud's object storage (Cloud Storage) is priced at $0.026/GB/month for standard storage, compared to AWS S3's $0.033/GB/month—offering ~20% savings.
- **Bandwidth Savings:** Google's egress fees get cheaper with usage while AWS's fees get more expensive, reducing costs for transferring large volumes of data—a critical factor for CrowdStrike's real-time monitoring and analytics.

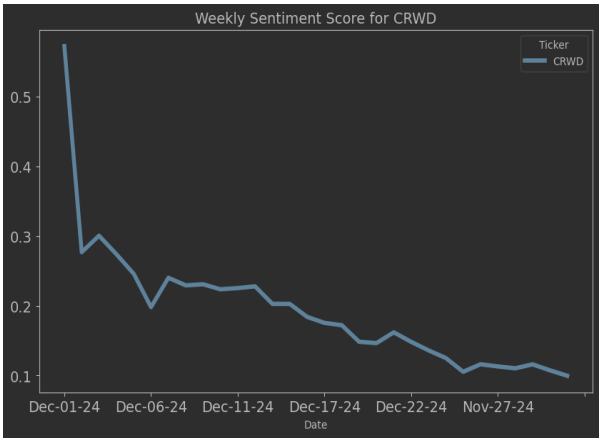
Scale Economies: As CrowdStrike scales, we expect its COGS as a percentage of sales to decline from 24% (FY23) to around 19% by FY27, driven by scale economies and better cloud cost management.
Key Bet: We forecast a 350 bps gross margin expansion by 2028, resulting in a ~$300M EBITDA in FY 2028 uplift not fully captured by the Street's estimates.

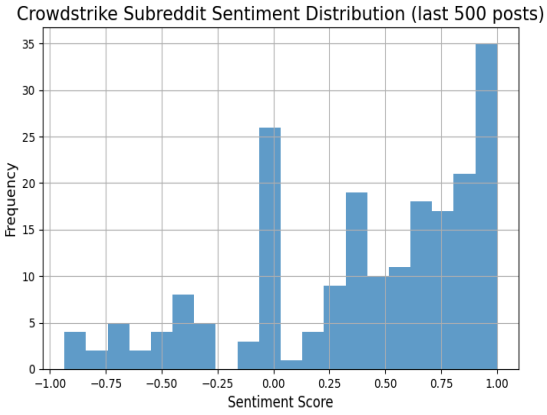
3) Market Touch Too Bearish on CrowdStrike Product Offerings Post-Outage
Our sentiment analysis highlights a notable divergence between market/media sentiment and actual customer sentiment regarding CrowdStrike's product offerings in the aftermath of the outage. While sentiment initially plummeted, recovery has been steady, with customer feedback currently indicating a significantly more favorable perception when compared to traditional media and investor perception.

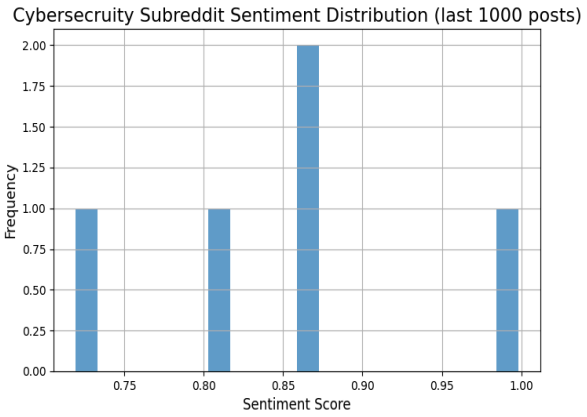
Analysis Insights:

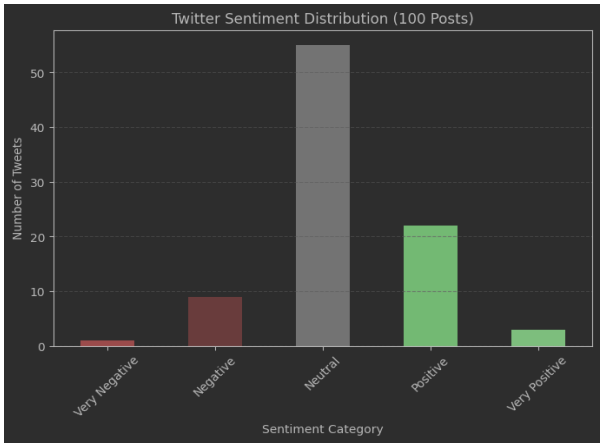
1. **Sentiment Analysis Across Data Sources:**
    - **Traditional Media:**
        - During the week of December 1, 2024, the average sentiment score in headline news articles was **+0.5** (categorized as "positive").
        - By December 27, 2024, sentiment declined to **+0.1** (categorized as "neutral"), reflecting a cautious and largely indifferent market stance toward CrowdStrike.
    - **Alternative Data (Customer Sentiment):**
        - Analysis of over 1,000 posts from the r/cybersecurity and r/crowdstrike subreddits, as well as Twitter mentions, shows a contrasting sentiment trend.
        - Customer sentiment consistently scored above **+0.25**, with over 50% of posts registering **+0.75** or higher (categorized as "extremely positive"), underscoring strong customer satisfaction and positive user experience.
2. **Event Sentiment Analysis:**
    - Reviewing over 100,000 events tied to CrowdStrike – including earnings reports, news, and product announcements – reveals a sharp sentiment drop immediately following the outage but has since rebounded to its historical average, suggesting a normalization in perceptions over time.

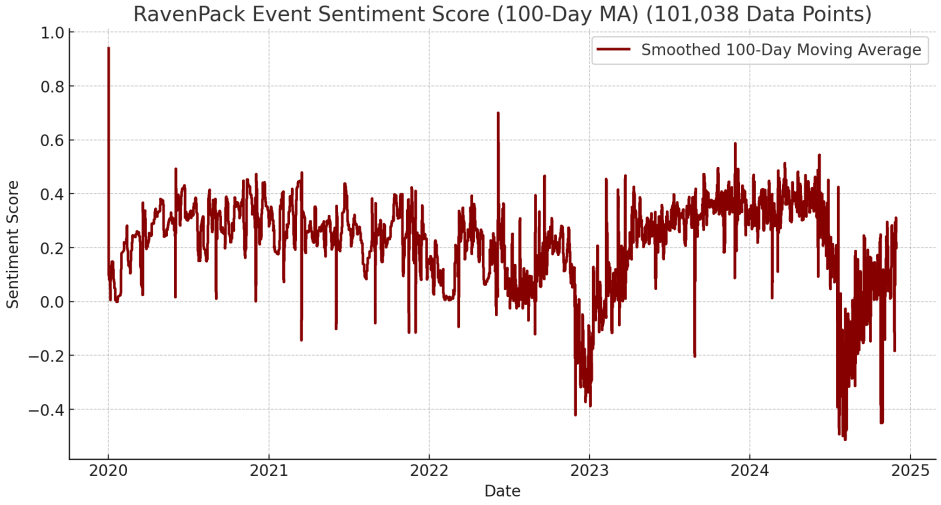
Key Bet: We believe that the market is a touch too bearish relative to what actual users think and what broader customer sentiment suggests. As a result, we think in the short term there could potentially be a 5-10% movement back to where the stock was trading prior to the outage.











Valuation:

We derive a 2024E price target of ~$315 (~10% downside) using a DCF approach.

DCF Valuation: 10-year projection with 8.75% WACC, ~25-30% CAGR in FCF with a terminal growth rate of 3%. We recommend a Hold on this opportunity.

Risks & Mitigants:

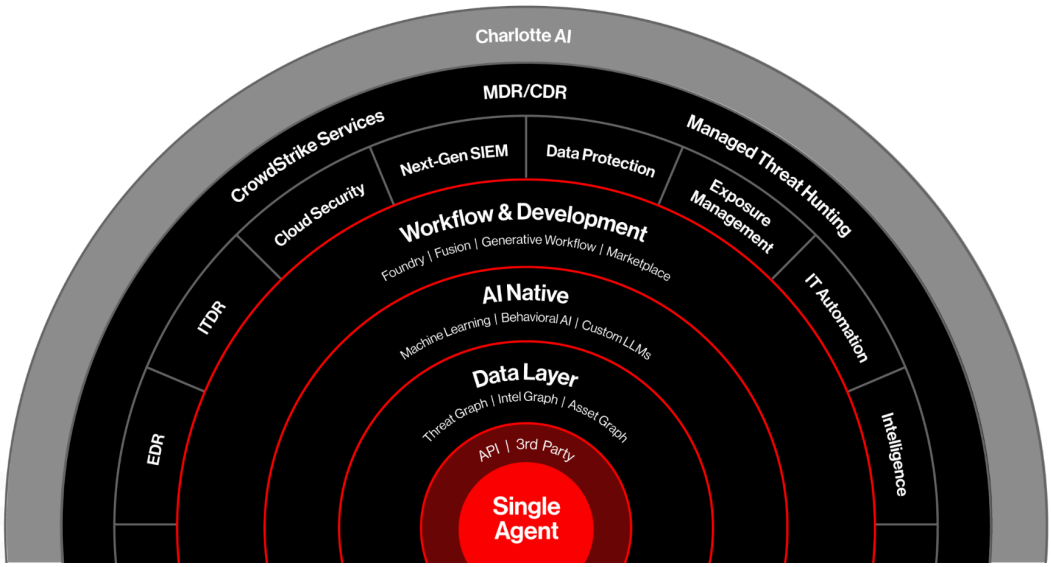
1) Competition from Legacy Providers: CrowdStrike faces competition from other legacy players like SentinelOne, Palo Alto Networks, and Microsoft Defender. However, CrowdStrike's modular cloud- and AI-native platform offers the flexibility and scalability that legacy solutions lack.
2) Regulatory Challenges: Compliance with global data privacy laws (e.g., GDPR) poses a risk. However, CrowdStrike's proactive investments in compliance and data protection mitigate this risk.
3) Economic Downturn Impact: Budget cuts in IT spending during a recession could impact CrowdStrike's growth. However, cybersecurity remains a top priority, especially given the rise in sophisticated cyber threats.

Catalysts:

1) Q1 FY 2026 Earnings Report: Expected demonstration of cloud cost efficiencies and margin expansion.
2) Continued Expansion into New Modules: New product launches in identity protection and threat intelligence will drive cross-selling.
3) Strategic Partnerships: Further cloud cost optimizations through deeper integration with Google Cloud.

Appendix

Product Offerings



Pros:

1) I work in cloud security and I've worked with a few of the EDRs, so I can offer some info on this: Falcon's detection-rate is unmatched pretty much across the board. We had a Red Team exercise where they gave up before they could even get the payload code onto the machine, much less execute it; it threw off detections even if they tried to write the code on the machine itself. It is really, really good at preventing lateral movement in the network, even assuming an employee manages to get phished. Far fewer false-positives than S1 as well; we moved away from S1 because it took our developer environments down too often, setting Exclusions didn't always wo rk due to bugs in the Exclusion logic, their guidance to us was just to use very broad exclusions and we were not satisfied with that answer.

   Falcon's UX/UI is really nice to work with. Defender moves shit around super often, every quarter you're learning new names for features and figuring out where everything was moved to. S1 wasn't as bad as Defender on this front, but they also had a habit of changing stuff around more often than we'd like.

   Falcon's reports can output eye-candy for leadership with pretty minimal tweaks. Very easy to present and manage

2) Overall CS caught more threats than s1 and defender in our pov. They're easier to work with in regards to setting up and deployment. Our company doesn't plan on moving any time soon. It's not easy just to rip and replace. Hoping we don't after getting certs for cs. But overall it's the tech and experience is what customers should be aware of that is better than the competition out there. I can say for sure this won't happen again. If it does they're done for.

3) There are many organisations that have gone down this path, and lots of discussions regarding side-by-side comparisons that have been carried out. Your shop is probably too small to run a side-by-side so you'll have to rely on reporting from those that have. I can tell you that, hands down, CS was the clear winner. The detection rates were far higher, the FP rates far lower, the level of control and configurability is much better with CS. I'm snr in a 10 person SOC looking after 5.5k users and 12k endpoints, nix, win and mac workstations and servers. The FP rate when we had defender was terrible, it was always late (it would alert on something seen x hours ago!) and you had to do the login dance to the portal, navigation hell to get the event details. This slows down response times.

   It is without doubt the most accurate CMDB we have because we have it on every endpoint. Once you get into the APIs of cs, some real magic can happen. Automated response, triage, containment, RTR on a single or hundreds of hosts (batch-session). Recently used it to restart a hung service on 400 servers after a bad update left the service locked by an orphaned kennel hook, and the only way to recover was a service restart or a server reboot. Initiated a batch rtr session on all 400, execute pkill then systemctl restart command, 2 minutes later job was done.

   MS don't care about your tiny 1200 user base, CS does. Their support is excellent. If anything, ditch the E5+ licence cost, invest in upskilling your team and using the full capabilities of what you seat have in CS.

   I do not work for Crowdstrike, I just believe it is the best of breed and it keeps getting better with new capabilities coming online all the time.

4) So where we sort of differentiate or where CrowdStrike differentiates from the competition is that is a very lightweight agent and they'll talk about it in the IT, just in the IT language about endpoint or agent bloat. So every security functionality has some sort of agent. And they all seem to be lightweight. But the way that we've discovered and the

way that CrowdStrike has developed their endpoint agent, it is very lightweight, meaning it uses less than 1% of the CPU utilization.

5) Tegus(Cushman and Wakefield) So on the vendor selection side, we really talked to Symantec because they were the incumbent. And they were a little bit more cloud-ready, still not nearly where CrowdStrike was, but they had made some strides. We also looked at Microsoft, because we're a big Microsoft shop. So, you know, Microsoft's always pushing their ATP and, "Oh, you own part of this." And then, CrowdStrike. What we really did with that was a much deeper cost-benefit analysis. What's the operational cost for running Symantec and what we would have to do to get to the same outcomes? With CrowdStrike, the same thing and then with Microsoft. And really at the end of the day, the cost-benefit analysis showed that CrowdStrike was the best fit for us because it offered not necessarily the cheapest price, but it offered the best overall cost to operate.

   So that included not only licensing cost, but people cost, server systems, all of that sort of thing, the total cost of ownership at the end of the day.

Cons:

They’re gonna have to make concessions for a while to keep deals afloat. Their stock has a lot of growth priced in and this could send them tumbling further, but who knows at this point, it was already priced pretty ridiculous to begin with and tech stocks don’t really follow logic

They’re gonna have a tough time recruiting engineers for a while, but, their saving-grace might be that the job market isn’t great for engineering right now and even highly-skilled candidates may not have a lot of other options.

Their public PR sucks ass, so I expect their customer-loss will be concentrated amongst their smaller and mid-size customers, which is where they have a lot of room to grow.

Potential Other Theses

1) Post-COVID, as startups surge during COVID continue to develop in their lifecycle and move up to MM and upper-MM operational ranges, they begin investing in operational infrastructures including cybersecurity, which CRWD can capitalize on.
    a) Concerns—priced in already?
    b) Trying to find more data (numbers, how many new businesses)
    c) Potentially priced in because the stock is expensive and pricing in additional revenue growth
    d) Too hard to quantify…
2) Businesses trending toward consolidation (platformization) in SaaS (cybersecurity specifically); **CRWD activity in M&A** (e.g. recent acquisition of Adaptive Shield) allows them to gain and maintain market share and generate inorganic growth as they gain new revenue streams through those acquisitions.
    a) CRWD diversity and strength of product offerings; ease of use (John has above); ease of integration with other SaaS (because of cloud-nativity)
    b) "two-pronged" thesis with current thesis 1 ("Superior Technology & Operational Excellence as Competitive Moat")
    c) In general, **M&A typically tends to be value destructive** (on the avg), though some M&A can have upside; hard to make bets on the company doing more M&A in the future, but can work recent small-scale M&A into the models
    d) CRWD right now does have a pretty good platform in terms of having all products in one place; not sure of value in large-scale acquisitions
    e) CRWD is end-point focused (bread and butter) but lots more in cyber market beyond EDR; potentially decent room to grow by growing offerings
    f) Can we find a consistent pattern of M&A? Potential companies they could acquire? Can we articulate what will happen there?
        i) Articles! Pitchbook?
        ii) Previous acquisitions
            (1) Adaptive Shield (Nov 2024) – $300M
            (2) Flow Security (Mar 2024) – $96.4M
            (3) Bionic (Sept 2023) – $239M
            (4) Reposify (Oct 2022) – $18.9M
            (5) SecureCircle (Nov 2021) – $60.8M
            (6) Humio (Mar 2021) – $370.3M
        iii) Screen public companies in the cyber sector (adjacent to CRWD, potential buyout)
        iv) SentinelOne?

g) CRWD is in the business of software, not M&A—outside where they provide value; BUT if there is opportunity to cross-sell/upsell through M&A then maybe…

h) Model in return on invested capital on each acquisition; assume every acquisition is >9% ROIC

i) Find out historical multiple

ii) Model in X acquisitions at Y% ROIC

iii) With (for example) 12x multiple

iv) Very PE way of doing it (chuck a ROIC, chuck a multiple, hope it's correct) - modeling is "lipstick on a pig"

	CrowdStrike Holdings (NAS: CRWD)	Publicly Held	90,647.53
1	Cisco Systems (NAS: CSCO)	Publicly Held	233,469.29
2	International Business Machines (N...	Publicly Held	213,426.59
3	Palo Alto Networks (NAS: PANW)	Publicly Held	128,982.67
4	Snowflake (NYS: SNOW)	Publicly Held	55,343.00
5	Cloudflare (NYS: NET)	Publicly Held	38,986.83
6	Zscaler (NAS: ZS)	Publicly Held	30,463.70
7	Splunk	Acquired/Merged (O...	26,443.83
8	Check Point Software Technologies ...	Publicly Held	20,651.42
9	CyberArk Software (NAS: CYBR)	Publicly Held	15,446.02
10	Elastic (Database Software) (NYS: E...	Publicly Held	10,782.87
11	Proofpoint	Privately Held (backi...	10,159.62
12	SentinelOne (NYS: S)	Publicly Held	7,683.28
13	Qualys (NAS: QLYS)	Publicly Held	5,398.56
14	Mandiant	Acquired/Merged (O...	5,397.45
15	Tenable (NAS: TENB)	Publicly Held	4,997.63
16	Darktrace	Privately Held (backi...	4,938.65
17	McAfee	Privately Held (backi...	4,886.66
18	Rapid7 (NAS: RPD)	Publicly Held	2,508.67
19	SecureWorks (NAS: SCWX)	Publicly Held	753.79
20	Arctic Wolf	Privately Held (backi...	

3) CRWD was valued at $400 per share prior to the outage and nothing has fundamentally changed about the business or product since then, so there is still room for a further valuation increase.