BABSON
BABSON COLLEGE FUND

Initiating Coverage of CrowdStrike (CRWD)

The BCF is initiating coverage of CrowdStrike Holdings, Inc (NAS: CRWD) with a BUY rating and a price target of $225 (35% upside) derived from a 50/50 split on a relative and discounted-cash-flow valuation. If approved, the Information Technology team expects to allocate 5% of the IT portfolio to CRWD.

Investment Summary

1. The market underappreciates the degree to which recent secular trends in the cybersecurity industry, including the SEC's recent mandate that companies promptly disclose cybersecurity hacks, serve to boost CrowdStrike's top-line growth through expansion of the endpoint security industry.
2. CrowdStrike's comprehensive product suite and its focus on product integration will allow it to increase market share as enterprise and SMB customers seek to optimize their total cost of ownership through the remainder of 2023.
3. CrowdStrike's recent achievement of GAAP profitability highlights how the firm can sustain rapid top-line growth while simultaneously delivering earnings beats to investors, unlike many of its competitors.

CrowdStrike Holdings		
Company Name	CrowdStrike Holdings, Inc.	
Ticker	CRWD	
Exchange	NASDAQ	
Valuation Date	9/26/2023	
Author	Ian & Thames	
Valuation Summary		
	Price	% Weight
DCF	$243.3	50.0%
Relative Valuation	$207.0	50.0%
Base Target Price		$225.1
Current Share Price		$167.4
Upside		34.5%
Consensus Price Target		$195.0
Different from Consensus		15.5%
Fiscal Year End		1/31/2024
Currency		$
Denomination		Millions
Diluted Shares Outstanding (mn)		238.8
Total Debt (mn)		741.8
Preferred Stock (mn)		-
Minority Interest (mn)		31.9
Cash & Cash Equivalents (mn)		3,167.2
Market Capitalization (mn)		41,562.3
Enterprise Value (mn)		37,828.0

Rationale for Cybersecurity Exposure

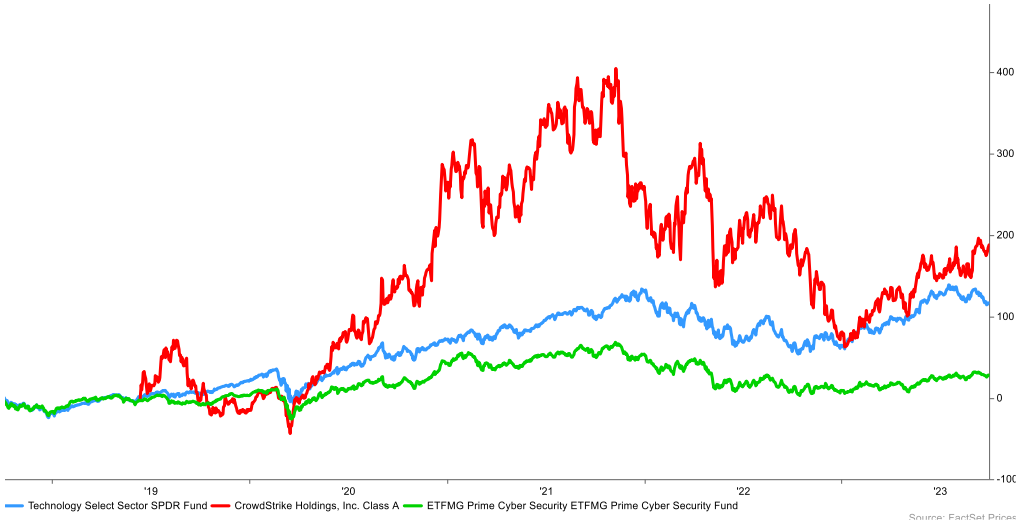
Out of the three major IT sectors (hardware, semiconductors, and software), the BCF is most bullish on software, given its network effects, high barriers to entry, and the generative AI (GenAI) catalyst. Within the software sub-sector, we believe that consolidated enterprise, cybersecurity, and infrastructure software stand to gain the most in 2H23.

Fueled largely by the 2023 rate hikes, SMBs and enterprise customers have pulled back their spending on superfluous software applications, creating a demand headwind for software firms whose 2022 wave has crested. Per Bloomberg, several of the smaller, high-growth companies of 2022, including Snowflake, Datadog, MongoDB, Palantir, Atlassian, Twilio, and Zoom are at risk of top-line estimate cuts given the recent correction for their customers' overspending in 2022.

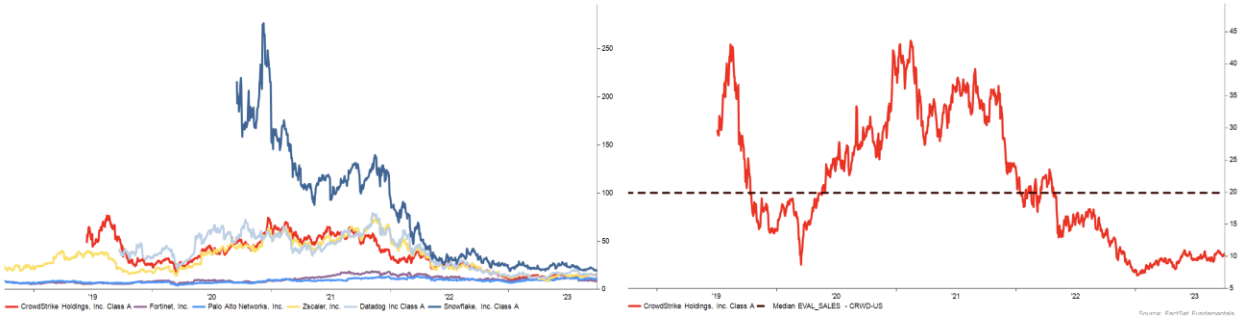
Large-scale, enterprise-level software firms will benefit from this environment as they provide consolidated suites of products that are attractive to companies looking to lower their total cost of ownership (TCO). Infrastructure, cybersecurity, and engineering software similarly stand to gain due to their high switching cost and competitive moat that make them resilient to weakening demand. Out of

these options, several secular trends motivate us to be the most bullish on cybersecurity. The SEC introduced a requirement in July 2023 that publicly traded firms disclose material cybersecurity hacks within four days of occurrence with a Form 8-K. These new reporting standards have already underscored the vulnerability of firms like Clorox and MGM, who were subject to cybersecurity attacks in mid-August and early-September, respectively. The full breadth of the SEC's new reporting and internal mandates will become effective on December 15, 2023, and we expect them to accentuate the urgency of integrated endpoint security by notifying investors of firms' vulnerabilities and sources of potential material financial impact. Firms have already started to preempt the regulations by reevaluating whether their legacy cyber stacks will suffice, creating a clear catalyst for the last three months of 2023.
CrowdStrike is the natural selection given these secular trends. CrowdStrike derives its competitive advantage from its integrated breadth of modern cloud security products, which allows its clients to consolidate their existing cyber stacks to reduce their total cost of ownership. The cost-cutting trend among software clients in 2023 serves to benefit CrowdStrike since clients can consolidate their infrastructure and reduce their cybersecurity-related expense by migrating to CrowdStrike's platform. High-profile cyber-attacks and the SEC's recent regulations regarding novel disclosures will also serve to benefit the cybersecurity industry. In addition to its competitive advantage, we believe that CrowdStrike is attractively priced at 10.7x EV/NTM Revenue compared to its peers and its own trading history.

[Figure 1] CrowdStrike vs. XLK vs. HACK (Cyber ETF) Indexed Share Price



[Figure 2] CrowdStrike vs. Peers EV/NTM Revenue; CrowdStrike EV/NTM Revenue



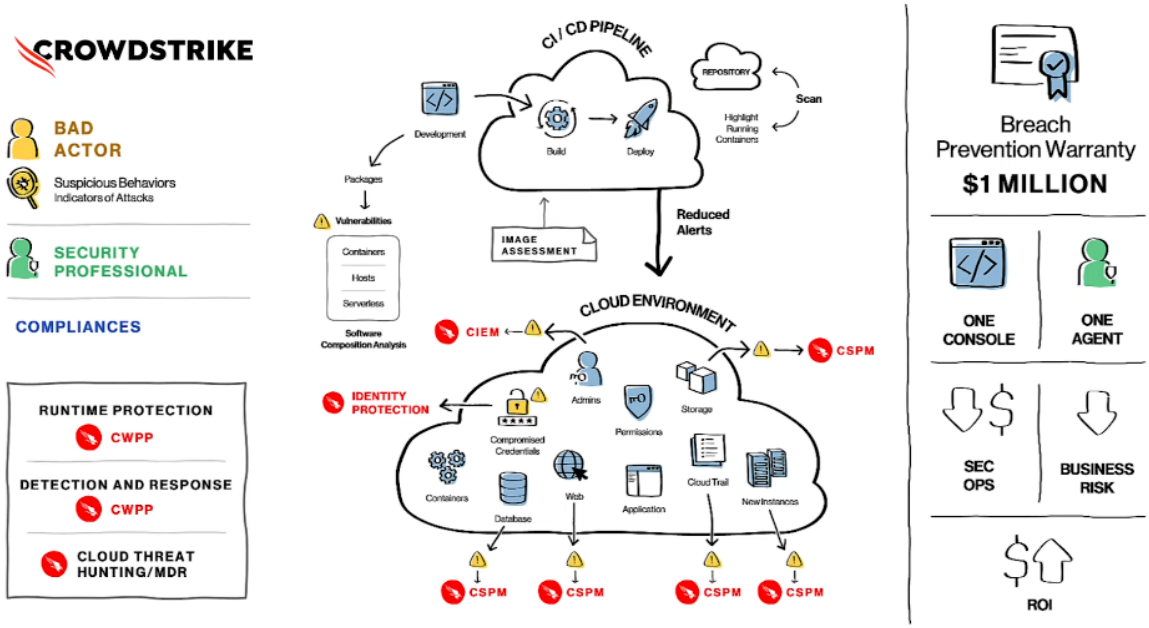
CrowdStrike Company Overview

CrowdStrike is a leading next-generation cybersecurity software company founded in 2011 that first listed on the Nasdaq in 2019. CrowdStrike's Falcon platform focuses on endpoint protection, threat intelligence, response services, and firewall management. When it was founded in 2011, CrowdStrike was the pioneer for cloud-native cybersecurity and briskly outperformed legacy systems that either refused to adopt cloud technology altogether or performed poorly after being haphazardly migrated to cloud servers. CrowdStrike's single, lightweight agent (the app downloaded onto endpoint devices—phones, computers, servers, etc.) consolidates detection and prevention capabilities to streamline sources of data, AI optimization, and decision-making tools allowing data to be automatically used for multiple use cases, unlike its legacy counterparts.

CrowdStrike uses advanced technologies like predictive AI and machine learning to detect and prevent cyber threats before they can infiltrate an endpoint device. The company is well positioned to continue to grow in the fast-growing cybersecurity market, driven by its innovative products and services, strong customer relationships, and a talented team of cybersecurity experts. The elevated-interest-rate environment during 1H23 that we forecast will extend into 2024 has caused many SMBs and enterprises to cut back on superfluous features for their software tech stacks which were purchased during the tech run of 2021-2022. However, integrated cybersecurity software has only grown more important and more attractive during the same period, reflecting its resilience to hiked-rate-fueled uncertainty.

While CrowdStrike's business model resembles the simple business models of other SaaS (Software-as-a-Service) and PaaS (Platform-as-a-Service) companies, the mechanisms behind its technologies are difficult to comprehend for the average investor. Figure 3 is a diagram used by CrowdStrike to explain to outsiders how its platform serves its clients. Each blue icon represents an element of a client's cyberspace that is either directly or indirectly vulnerable to exploitation by a bad actor. The red nodes are cybersecurity products offered by CrowdStrike that address each of these vulnerabilities. Rather than make a futile attempt to comprehensibly explain how each of these technologies operate, we wish only to highlight the comprehensiveness of the product suite that serves as CrowdStrike's competitive advantage. Each product (the red nodes) serves as a source of data for CrowdStrike's Threat Graph, which amalgamates all bad-actor data to improve CrowdStrike's predictive abilities over time. As a result, the integration between products creates cross-synergies that improve the platform's performance.

[Figure 3] CrowdStrike Product Offerings (source: CrowdStrike)



Cloud-Native Architecture

CrowdStrike's Falcon platform is the first to be built entirely in the cloud, giving it an edge over legacy cybersecurity platforms that were migrated to the cloud after their inception. Falcon's cloud-native architecture enables the collection and analysis of large-scale, crowdsourced data from all its historical clients to help predict and preempt future breaches. The cloud allows CrowdStrike's platform to be lightweight, resilient, and high performing, facilitating the user experience and the protection of clients' workloads on a variety of diverse endpoints (phones, laptops, company servers, etc.); the Falcon agent takes up less than 35 MB of hard drive space and works on Windows, macOS, Linux, and other common operating systems.

Falcon Agent

CrowdStrike's Falcon agent is a lightweight intelligent application installed on each CrowdStrike endpoint and cloud device. The streamlined application allows for the identification and prevention of known threats (malware and non-malware), machine learning to predict novel threats, and advanced behavioral techniques to develop efficient solutions for incident response teams within client firms. The agent can be installed on generic Windows, macOS, and Linux-run devices, making CRWD's Falcon platform accessible to many SMBs that do not have their own native architecture. The Falcon Agent sets CrowdStrike apart from competitors as CrowdStrike is "the only EDR [Endpoint Detection and Response] out there right now, which has good product parity on all operating systems" according to the Chief Information Security Officer at TripAdvisor.

The Falcon agent operates by correlating an event with a model of historical threats and incidents, analyzing the event via agent-based machine learning, and automatically implementing preventative and diagnostic actions on the individual endpoint device. The agent can also be remotely configured in real

time based on intelligence from the cloud. In contrast to other legacy systems and competitors' platforms (e.g. Zscaler), CrowdStrike's Falcon agent consolidates the functions typically performed remotely in the cloud into the single endpoint where the event is identified. This allows the Falcon agent and platform to take diagnostic and preventative measures on the endpoint device without having to relay a situational description to the cloud, expediting response times compared to competitors.

Threat Graph

CrowdStrike's database consists of a proprietary and dynamic threat graph that continuously searches for malicious activity using predictive AI with pattern-matching techniques. CrowdStrike's proprietary technology allows it to combine the historical data collected through its graph analytics and AI algorithms to enrich the collected data from third-party intelligence. The graph model allows the machine learning algorithm to identify relationships between events that are not ostensibly related, yielding valuable insights into potential future attack patterns. CrowdStrike's AI algorithms are advantaged by the rich proprietary dataset the firm has collected since its inception, which also serves as a barrier to entry for cloud cybersecurity competitors.

Intel Graph & Asset Graph

Intel Graph is CrowdStrike's application for analyzing and correlating the massive amounts of data its endpoints collect on security adversaries and their strategies. CrowdStrike's pioneering industry position over the past decade has allowed to it amalgamate enough data to provide unrivaled insights and diagnoses regarding adversarial tactics and techniques.

Asset Graph is more passive as it monitors and tracks the interactions among clients' internal assets to assess adversarial risk on a real-time basis. Asset graph outputs a visualization of the relationship among all endpoints and assets, which include devices, users, accounts, and cloud workloads.

APIs and Integrations

Falcon's APIs give clients the opportunity to efficiently and effectively complement CrowdStrike's native software product offerings with security information event management (SIEMs), intrusion prevention systems, and intrusion detection systems. APIs and integrations add a level of customizability to CrowdStrike's tech stack offering that allows the platform to appeal to a greater market. These APIs also allow clients to connect their existing (non-Falcon) security systems to the Falcon platform, which has served in the past as a valuable land-and-expand strategy for CrowdStrike's top-line development. Existing customers who choose to add APIs and integrations from the CrowdStrike Store end up boosting CrowdStrike's top line while CrowdStrike incurs no incremental operating costs beyond overhead, leading to bottom-line improvements as well.

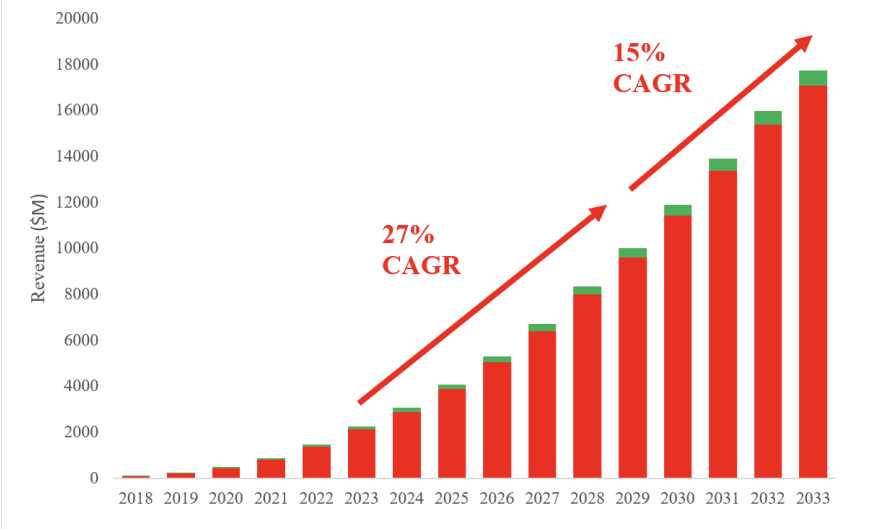
Revenue Segments

CrowdStrike divides its revenue into two segments: Subscription Revenue and Professional Services Revenue. Subscription Revenue (94.2% of the total in FY23) consists of subscription fees for the Falcon platform and additional cloud modules that are supported by the cloud-based system. Subscription Revenue is primarily driven by the number of subscription customers, number of endpoints per customer, and the number of cloud modules included in the individual subscription plan. Most Subscription Revenue is billed upfront and recognized ratably over the contract term of 1-3 years, causing the firm to

sustain a significant deferred revenue balance. Subscription Revenue is only billed to multi-year-contract clients at the beginning of each year of their contract, so the firm maintains a sizeable balance of receivables as well.

Professional Services Revenue (5.8% of the total in FY23) consists of incident response, proactive services, forensic and malware analysis, and attribution analysis services that CrowdStrike provides to clients separately from subscriptions. Professional Services are available through an hourly rate or fixed-fee contracts for non-subscribers, and Professional Services clients frequently become new Subscription Revenue clients, reinforcing the firm's land-and-expand strategy. Professional Services revenue is recognized as the services are performed.

[Figure 4] Revenue by Segment (Subscription vs. Professional Services)



Industry Overview & Secular Trends

Growth of Cyber Threats

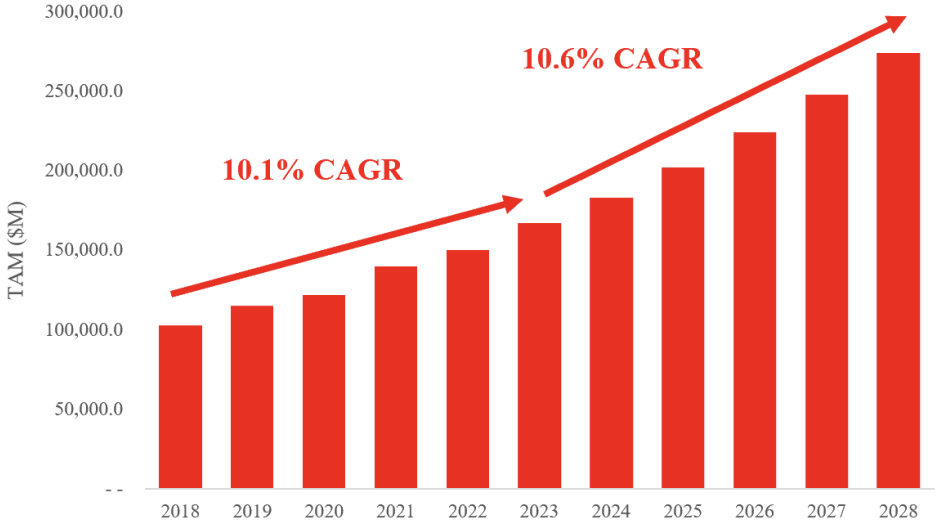
Threats to firms' cybersecurity have only grown more common and sophisticated since CrowdStrike launched its Falcon platform. Targets now face heightened attacks from well-funded nation-states, technically equipped criminal organizations, and hackers who can easily access advanced methods of cyberattack. The typical attack cycle starts when an attacker attempts to penetrate an endpoint device (computer, laptop, server, etc.) to establish a beachhead. The bad actor then can steal and exploit legitimate credentials, escalate their privileges, and move laterally within the target's program to escalate the attack. At this point, they can install malware or ransomware, or they can encrypt, destroy, or silently exfiltrate sensitive data.

Since Covid-19, organizations have embraced the digital transformation, adopting more cloud-based services, increasing the mobility of their workforce, and growing the number of interconnected devices on their networks. Without an integrated cybersecurity solution, the digitalization trend exposes an increasingly broad attack surface to adversaries.

Need to Reduce Complexity and Simplify Security Operations

Given the hiked-rate environment and the subsequent spending cuts heading into 2024 among many SMBs and enterprise clients, organizations are increasingly looking to reduce the complexity of their tech stacks, in particular their cybersecurity infrastructure. Reducing the complexity of the overall cybersecurity network reduces total cost of ownership, making consolidation particularly appealing for the last three months of 2023. Modern security systems are also better optimized the fewer point products, agents, and technologies that they implement. CrowdStrike's management indicated in its 2Q24 earnings call that consolidating cybersecurity infrastructure has reduced costs for major construction clients by up to 60%, highlighting the appeal of CrowdStrike's platform given the need for simplification and the macro headwinds for 2024. Ending ARR for Falcon Modules grew to $296M in FY23 from one year prior, representing a 70% increase year-over-year and reinforcing clients' emphasis on consolidation spend.

[Figure 5] Cybersecurity Total Addressable Market (2018-2028) per Gartner



Thesis 1

The market underappreciates the degree to which recent secular trends in the cybersecurity industry, including the SEC's recent mandate that companies promptly disclose cybersecurity hacks, serve to boost CrowdStrike's top-line growth through expansion of the endpoint security industry.

Per Gartner, the cybersecurity total addressable market grew at a 11% five-year CAGR from 2017 to 2022 (from $90B to $150B). From 2022 until 2027, the TAM is expected to continue at a similar pace of 10.5% CAGR from $150B to $250B. CrowdStrike's market share of the comprehensive cybersecurity TAM has grown thirteenfold from 0.1% to 1.3% between 2018 and 2022. Consensus estimates for revenue growth expect CrowdStrike's market share of total cybersecurity to grow from 1.3% to 2.9% between FY24 and FY28. We forecast that the growth of the endpoint security industry will accelerate further as companies face pressure from federal and state governments. In July 2023, the U.S. Securities and Exchange Commission adopted regulations requiring firms to disclose in their Form 10-K Annual Reports their efforts to preempt cyberattacks and mitigate their risk. Given that CrowdStrike had a 22.2% market-

leading share in the endpoint-security market and was ranked #1 out of 26 endpoint security vendors by IDC, we believe that CrowdStrike stands to gain the most from the new SEC policies. The new regulations require firms to disclose on their Form 8-K the new Item 1.05 with a discussion of any cybersecurity incident deemed to be material and to describe the attack's nature and scope. On the Form 10-K annual report, firms will have to describe their internal processes for preempting cybersecurity threats in the new Item 106.

We forecast that the increased transparency required by the new SEC disclosure requirements will pressure firms to increase their spend on cybersecurity and migrate from legacy, outdated cybersecurity platforms to modern, endpoint security solutions. CrowdStrike historically has had two on-ramps for top-line growth: clients who have never had a concrete cybersecurity system deciding to purchase CrowdStrike's platform and clients who previously used a legacy system deciding to upgrade to CrowdStrike's superior integrated suite. We expect the new SEC guidelines to have a material impact on the second type of client (the "upgraders"), given that we expect investors to be increasingly hawkish on the status of their investment companies' cyber stacks following the new transparency requirements. Consensus estimates that the endpoint security industry's TAM will rise from $13.7B, or 7.5% of the total cybersecurity industry's TAM, to $23.8B, or 8.7% of the total cybersecurity's TAM, between 2024 and 2028. Our projects differ from consensus in that we expect endpoint security's TAM to rise from 7.5% to 10% ($27.4B) of the total cybersecurity market's TAM by 2028. Since CrowdStrike is the market leader in the endpoint security space, it stands to gain the most from our assumption, especially when coupled with our forecasted market share increases (Thesis #2).

Thesis 2

CrowdStrike's comprehensive product suite and its focus on product integration will allow it to increase market share as enterprise and SMB customers seek to optimize their total cost of ownership through the remainder of 2023.

Although CrowdStrike initially began as a provider of endpoint security, the company has expanded its offerings to include 27 cloud modules on their single Falcon platform that cover multiple important security markets, including security and IT operations, managed security services, observability, cloud security, identity protection, threat intelligence, data protection and cybersecurity generative AI. CrowdStrike's modules can be instantly added to a customer's modules through CrowdStrike's SaaS model. Additionally, clients adding Falcon modules end up boosting CrowdStrike's top and bottom line, given that the incremental operating expense is only allocated overhead.

CrowdStrike's comprehensive product suite provides multiple advantages for clients including cost savings through their bundled offerings, increased efficiency due to CrowdStrike's single agent platform, and reduced complexity for the client's IT systems. According to our interview with Babson College's IT Security Engineer, many corporations currently use multiple vendors for different aspects of IT security services resulting in higher overall costs, lack of integration, high performance impact on the organization's systems due to having to run multiple software concurrently, and complex GUIs increasing the workload and labor costs for corporates to manage their IT systems. CrowdStrike's management indicated in its 2Q24 earnings call that several of the enterprise customers who transitioned to CrowdStrike's platform during the previous quarter used north of 60 cybersecurity point products.

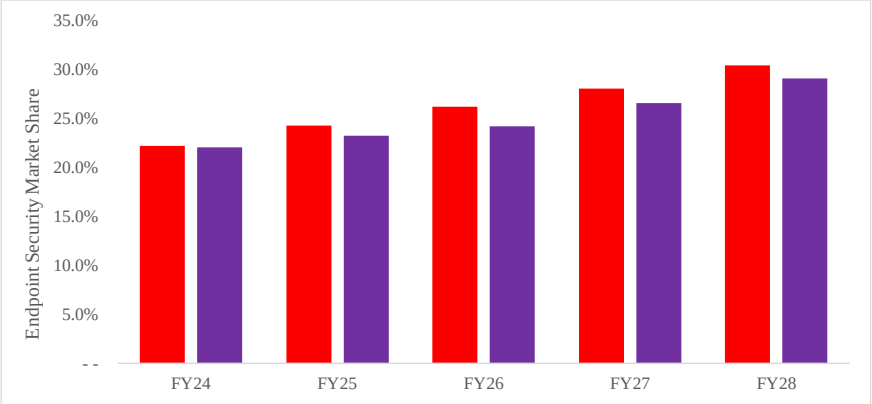
Consolidating their cybersecurity network with CrowdStrike resulted in a 60% improvement in total cost of ownership.

Based on our primary research, CrowdStrike's platform has several key advantages over its direct competitors', including Fortinet (FTNT), Palo Alto Networks (PANW), Zscaler (ZS), SentinelOne (S), Okta (OKTA), and Microsoft Defender. Babson's IT department chose to use CarbonBlack, a VMWare (VMW) platform based on a recommendation from its consulting company given a very short timeframe to decide on a platform. However, Jackob Backman, Babson's IT Security Engineer, explained that CrowdStrike is a superior platform than CarbonBlack, Fortinet, Palo Alto, and Zscaler due to its ease of deployment, simple user interface (UI), and lightweight agent. He emphasized how important CrowdStrike's superior UI will likely be in appealing to clients who do not have advanced existing cybersecurity infrastructure. We agree that the simplicity of the UI will be invaluable, especially as CrowdStrike targets more SMBs rather than enterprise clients over the next few years as management has suggested.

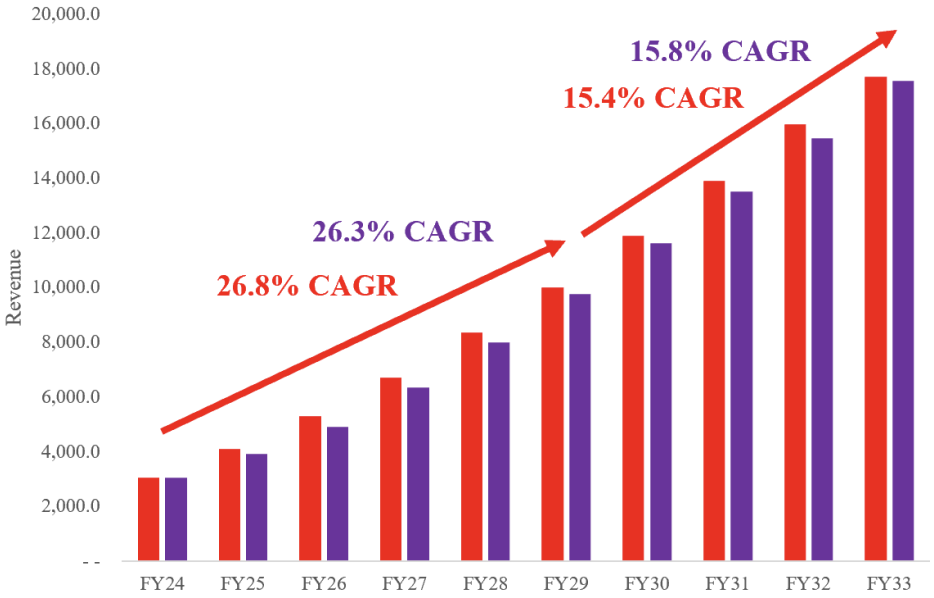
The advantage of Microsoft Defender and other legacy systems like Palo Alto Networks and Cisco (CSCO) is their existing physical cloud infrastructure (i.e., servers). Yet, we do not see the legacy systems benefitting for much longer, given CrowdStrike's recent investment in server infrastructure through its elevated Capex (10.5% of revenue in FY23 vs. 7.7% in FY22), to combat the hardware-based advantage of legacy systems, as well as the platform's reliance on Amazon Web Services (AWS) servers. We expect Capex to remain slightly elevated while it tapers down to a long-term rate of 4.5% in FY27. Our discussion with Babson's IT Engineer corroborated what CrowdStrike's management claimed about Microsoft Defender's clunkiness and lack of consolidation, as Jacob Backman emphasized the complexity of Microsoft's licensing structure and the disjointedness of its individual products.

Our analysis of CrowdStrike's superior offering leads us to believe that CrowdStrike will capture a greater portion of the endpoint security market than consensus forecasts. Our assumptions fall in line with the consensus revenue for the remainder of FY23, during which CrowdStrike's forecasted revenue of $3,057M implies a market share of 22.3% of the endpoint security TAM. However, we forecast that CrowdStrike will gain an additional 1.3% of market share beyond consensus estimates by FY28, yielding a 30.5% total endpoint security market share in FY28 vs. a 29.2% market share as forecast by consensus. Our resultant revenue five-year CAGR is 26.8% vs. 26.3% for consensus (between FY24-FY29).

[Figure 6] CrowdStrike Endpoint Security Market Share (BCF vs. Consensus)



[Figure 7] CrowdStrike Revenue Forecast (BCF vs. Consensus)



Thesis 3

CrowdStrike's recent achievement of GAAP profitability highlights how the firm can sustain rapid top-line growth while simultaneously delivering earnings beats to investors, unlike many of its competitors.

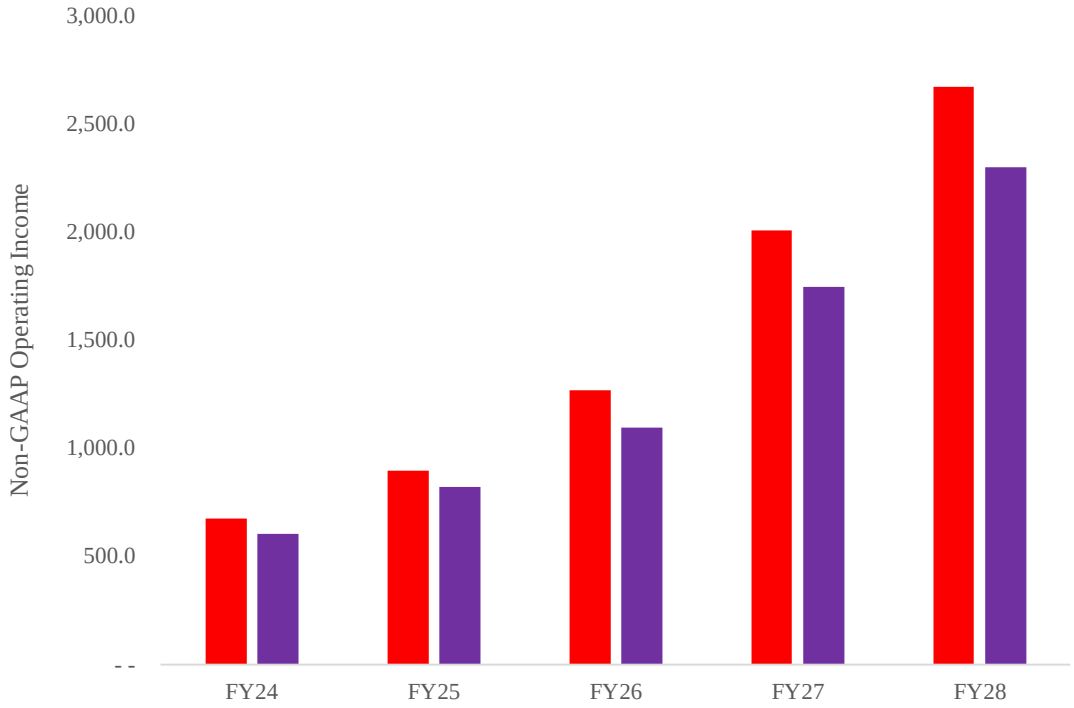
We believe that there are plenty of opportunities that will allow CrowdStrike to sustain its revenue growth, including focusing its sales and marketing to SMBs, launching new cloud modules, and its continued secular growth as the market continues to shift from legacy antivirus players to CrowdStrike's leading cloud-native solutions.

Simultaneously, CrowdStrike has several key catalysts to its bottom-line that distinguish it from its competitors. Namely, CrowdStrike's professional services, module-based platform, and the CrowdStrike Store all serve as on-ramps for top-line growth that minimize incremental sales and marketing expenditure. CrowdStrike's professional services offering includes incident response and forensic investigatory services, technical assessment and strategic advisory services, training for organizations that have experienced a cybersecurity breach, and assessment of clients' security posture and ability to respond to breaches. Professional services revenue remains a small proportion of CrowdStrike's overall revenue (5.8% in FY23), and revenue is billed at an hourly or contracted rate. Despite the low proportion of overall revenue, professional services clients typically end up entering subscription contracts to use CrowdStrike's platform after benefitting from its professional services counsel. Subscription revenue sourced from previous professional services clients represents high-margin top-line growth that will benefit CrowdStrike's bottom line, given that the only material operating expense associated with onboarding previous professional services clients is allocated overhead.

Similarly, the modular framework of CrowdStrike's subscription Falcon platform allows clients to add functionality like threat hunting, malware analysis, and firewall management to their existing cyber stacks. The cost of revenue associated with additional modules comes from the amalgamation and analysis of customers' data. Since the same endpoint devices use the modules as the baseline CrowdStrike Falcon platform, the incremental cost of revenue and operating expense from increased modules is minimal (i.e., allocated overhead), improving CrowdStrike's bottom line. In addition, the CrowdStrike Store is CrowdStrike's platform-as-a-service (PaaS) for third-party trusted cybersecurity apps. Once third-party applications are approved, they act much the same was as CrowdStrike's native modules—contributing top-line growth without materially increasing operating expenses. The significance of CrowdStrike modules and third-party apps is evidenced by CrowdStrike's 125.3% dollar-based net retention rate and gross retention rate of 98% in FY23, suggesting that 27.3% of CrowdStrike's FY23 revenue was driven by high-margin modules and third-party apps.

To model CrowdStrike's margin expansion, we forecast that CrowdStrike will achieve non-GAAP operating margins (includes an add-back for stock-based compensation and other irregularities) of 30% by FY28 and 40% at maturity by FY33. We are confident in this aggressive assumption given CrowdStrike's recent achievement of 22% non-GAAP operating margin in 2Q24, two quarters in advance of management's guidance. Consensus forecasts that non-GAAP operating margin will reach 28.8% in FY28 and does not guide for FY33, so our estimate differs from consensus by 1.2%. Our assumptions regarding improvements in operating margin stem from increased GAAP gross margin, which we anticipate will expand to 80% of revenue at maturity (FY33) and declines in sales and marketing expense to reach 24% of revenue at maturity (FY33).

[Figure 8] CrowdStrike Non-GAAP Operating Income Forecast (BCF vs. Consensus)



Valuation

Our weighted average price target of $225 is derived from a 50/50 split on a relative and discounted-cash-flow valuation. Through our benchmarking process, we ranked CrowdStrike in the 60th percentile among its cybersecurity and software peers. We elected to use an EV/NTM Revenue multiple for our relative valuation in line with industry trends, as well as because several peers are unprofitable. Our relative valuation suggests an 11.5x multiple be applied to our forecast for CrowdStrike's NTM Revenue, yielding an enterprise value of $47.0B and a share price of $207 (upside of 23.6%)

Our DCF employs a terminal growth rate of 2.5% and a WACC of 10.2%. Our WACC is derived from the tax-affected interest rate on CrowdStrike's only tranche of senior debt for the cost of debt. For the cost of equity, we used a 365-day daily market beta, 4-year monthly market beta, and a bottoms-up beta based on CrowdStrike's peers. We assigned a 60% weight to the bottoms-up beta (1.22), due to the unusually low results from the 365-day beta (0.98) and the 4-year beta (0.86). Our final beta is 1.10 and our WACC is 10.2%. For our exit multiple, we applied an EV/NTM Revenue multiple to our terminal year projected revenue forecast. We selected a multiple of 8.0x at a discount to CrowdStrike's current EV/NTM Revenue multiple of 10.7x to reflect our expectation that CrowdStrike will trade at a lower multiple in the coming year as growth slows. Our selected multiples for our relative valuation and exit multiple method both seem reasonable, given CrowdStrike has traded at much higher levels in the recent past (see Figure 2). Our 50/50 split between the terminal growth method and exit multiple method yields a price target of $243.3 (45% upside).

Catalysts

Corporate Cyber Security Attacks Raises Demand for Advanced Endpoint Security Protection
High profile corporate cybersecurity incidents including the recent cyber breach on MGM Resorts in September which impacted MGM's operations for over 10 days results in corporates looking to improve their cybersecurity protection resulting in higher demand for CrowdStrike's platform.

TAM Expands Faster Than Expected Due to Product Innovation and A Faster Shift from Legacy Players Towards Next-Gen Platforms
As CrowdStrike diversifies its services by adding new cloud modules, their total addressable market also increases. Furthermore, as companies go through their cloud transformation, we may see an accelerated share-shift from legacy antivirus players towards next-gen cloud native platforms like CrowdStrike.

S&P500 Inclusion
CrowdStrike became GAAP profitable in the past two quarters. The company needs to remain profitable for another two quarters to be eligible for index inclusion. We believe that Index Inclusion will be a catalyst for CrowdStrike as it will attract investments from long-only investors.

Risks

Risk of Cyber Attack
As a cybersecurity provider, CrowdStrike is a constant target of cyberattacks and one breach on their platform could significantly damage their reputation. CrowdStrike has access to many clients' sensitive data and a data breach could harm CrowdStrike's credibility.

Intense Industry Competition from Larger IT Players
Although CrowdStrike is currently the number one player in endpoint protection in terms of performance and innovation, there are many competitors including Microsoft which has the financial resources to improve their own products or provide steep price discounts to draw clients away from CrowdStrike.

High Revenue Growth Expectations
CrowdStrike has experienced high revenue growth since its IPO in 2019, failure to maintain growth expectations could result in a negative outlook.

Management

George Kurtz (President, CEO, Co-Founder)
George Kurtz is a co-founder of CrowdStrike, serving as President and CEO since November 2011. Prior to CrowdStrike, he held executive roles at McAfee, Inc. from 2004 to 2011, including Executive VP and CTO. He founded Foundstone, Inc. in 1999, serving as CEO until its acquisition by McAfee in 2004. He holds a B.S. in Accounting from Seton Hall University

Burt Podbere (CFO)
Burt Podbere has been CrowdStrike's CFO since September 2015. He served as CFO at OpenDNS, Inc. from May 2014 to August 2015 and at Net Optics, Inc. from October 2011 to April 2014. He is also Treasurer and a board member for the CrowdStrike Foundation since November 2017. Burt Podbere is a Chartered Accountant with a B.A. from McGill University.

Shawn Henry (Chief Security Officer)

Shawn Henry is CrowdStrike's Chief Security Officer since March 2012. He also served as President of CrowdStrike Services from March 2012 to October 2022. Prior to his roles at CrowdStrike, he had a distinguished career with the FBI from 1987 to March 2012, culminating in his role as Executive Assistant Director of the FBI's Criminal, Cyber, Response, and Services Branch. Mr. Henry holds a B.B.A. from Hofstra University and an M.S. in Criminal Justice from Virginia Commonwealth University.

Michael Sentonas (President)

Michael Sentonas is CrowdStrike's President since March 2023, previously serving as the Chief Technology Officer from February 2020 and as Vice President, Technology Strategy from May 2016 to February 2020. Before joining CrowdStrike, he held various positions at McAfee Corp. from March 2004 to April 2016, including Chief Technology Officer – Security Connected from November 2013 to April 2016. Mr. Sentonas holds a bachelor's degree in computer science from Edith Cowan University, Western Australia.

Disclosures

BABSON
BABSON COLLEGE FUND

Babson College Fund

The Babson College Fund (BCF) is an academic program in which selected students manage a portion of the Babson College endowment. The program seeks to provide a rich educational experience through the development of investment research skills and the acquisition of equity analysis and portfolio management experience. Please visit http://cutler.babson.edu for more information.

Definition of Ratings

BUY: Expected to outperform the S&P 500 producing above average returns.
HOLD: Expected to perform in line with the S&P 500 producing average returns.
SELL: Expected to underperform the S&P 500 producing below average returns.

References

FactSet
Capital IQ
Thomson/Reuters Eikon
Bloomberg
Company Filings
Gartner
Tegus

Analysts

Ian Cass
icass1@babson.edu

Thames Tangitvet
mtangitvet1@babson.edu