CrowdStrike: Standing tall in crowded cybersecurity

In a NY Times oped in 2018, Zeynep Tufekci wrote, *"The early Internet was intended to connect people who already trusted one another, like academic researchers or military networks. It never had the robust security that today's global network needs. As the Internet went from a few thousand users to more than three billion, attempts to strengthen security were stymied because of cost, shortsightedness and competing interests. Connecting everyday objects to this shaky, insecure base will create the Internet of Hacked Things. This is irresponsible and potentially catastrophic."*

In July last year, Rob Vinall mentioned the following in his letter to investors, "*it is worth remembering that crises come in different shapes and sizes. This crisis impacted the physical world to the benefit of the online world. The opposite scenario is equally possibly. In fact, in January I wrote that the greatest longtail risk to the economy was from a virus… of the computer variety (so near to glory, and yet so far). I still believe a computer virus is a major risk and strongly recommend reading "Sandworm" by Andy Greenberg to get up-to-speed on how fragile the Internet is."*

As I spent the last month understanding the vulnerability of our online world, it is hard not to sense a tangible fear of catastrophe sometime in the future. Companies such as CrowdStrike are one of the strongest answers to such vulnerabilities. I must admit that the velocity in cybersecurity space is moving forward at a dizzying pace, especially for a generalist like me. I am grateful to MI Capital, Ryan Reeves, Muji, Liberty, Cleveland Rainmaker, and the internet (even if it's "fragile") to help me get up to speed.

Here is the outline for this month's deep dive:

Section 1 Mini-primer on endpoint security: Many readers may not be quite familiar with the historical and current context of endpoint security. I briefly discussed and left some helpful readings that you can explore further if you are interested.

Section 2 CrowdStrike business model: I explained CRWD's business model and how it makes money.

Section 3 Sizing up the opportunity: I outlined CRWD's TAM and commented on their potential in cloud security.

Section 4 Competitive dynamics: A detailed discussion on competitive dynamics among legacy incumbents, next generation security companies, Microsoft, and some current crop of startups is presented.

Section 5 Valuation and model assumptions: Model/implied expectations are discussed here.

Section 6 Management, capital allocation, and incentives: I opined on the management, and their compensation incentives in this section.

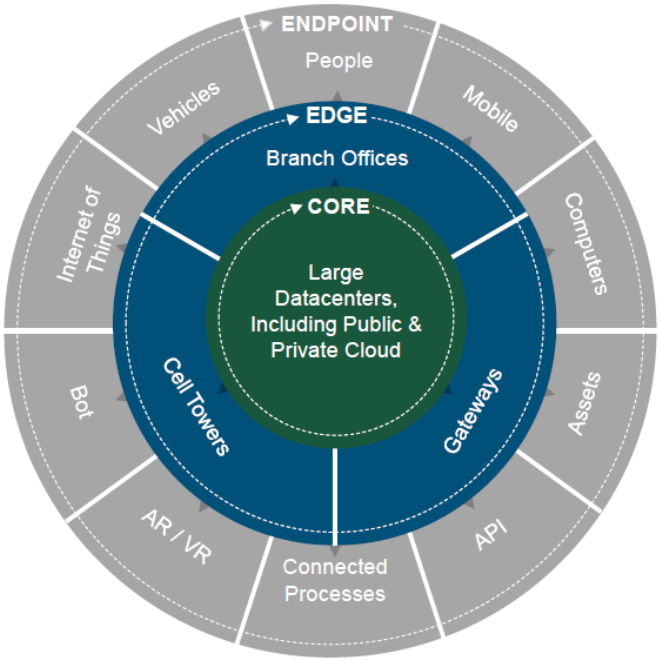
Section 7 Final Words: Concluding remarks on CrowdStrike, and brief discussion on my overall portfolio.

Section 1: Mini-primer on endpoint security

Unlike my previous deep dives, CRWD operates in an industry that is rather technical in nature which may make it difficult for many readers to connect quickly to the business. Therefore, I want to take a step back, and discuss the segment of the broader cybersecurity industry CRWD operates in before delving deep into CRWD's business. Given my non-technical background, I myself had to spend quite some time to understand the basics and historical context of the cybersecurity industry.

Since CRWD's core business is in endpoint security, let me start with what endpoint security is.

Endpoint is any device which can be connected to a network. Although most endpoints used to be desktops, laptops, and servers, many mobile devices such as smartphones, tablets, notebooks and even printers, cameras, Point of Sales (PoS) systems, and numerous other IoT devices are now within the scope of endpoint security. To visualize the endpoints in a typical network layout, just look at the below graph which I came across from Mary Meeker's 2019 presentation (Slide 152).



Source: Adapted from Graphics presented in IDC 'Digitization of the World From Edge to Core White Paper' developed in collaboration with Seagate (11/18), IDC DataSphere.

To understand how the endpoint security market evolved, we need to go back to 1987 when McAfee launched its first antivirus solutions, which was then followed by Symantec's antivirus solution in 1991. Antivirus is one of the components of endpoint security and its job is to prevent malware from encroaching its way to endpoint.

What is malware? Malware is a malicious and hidden software in a system/network that enables access to sensitive information for sabotage or espionage through methods such as attachments,

phishing, and even social engineering. Let me briefly elaborate the "social engineering" element to explain how people are extremely vulnerable to be hacked.

Inspired by a TV series "Mr. Robot", in 2016, some researchers dropped 300 malicious USB sticks on the University of Illinois Urbana-Champaign campus. 48% of the sticks were picked up, plugged into the computer, and had at least one file opened by people who found them. Since ~20% of the drives were connected within the first hour of dropping the sticks, you get a very short window to address such a security concern. There are lots of interesting findings and implications from this experiment which you can explore further here.

It is easy to understand why endpoint security has gained momentum when you understand the context of the legacy solution that it continues to replace. In early days of cybersecurity, antivirus-based legacy security solutions could only protect a system/network against malware attacks that have previously been identified as malicious and stored in a database. These reactive solutions are incredibly ineffective because by 2007, ~5.5 mn malware samples were identified in that year alone and by 2013, ~400k new malware samples were being reported every day. It was clear that signature-based databases could not possibly be updated at the rate of new malwares being created.

I could sense the terrible situation of cybersecurity when I read Gartner's report on End Point Protection (EPP) in 2016: *"when 44% of reference customers for EPP solutions have been successfully compromised, it is clear that the industry is failing in its primary goal: blocking malicious infections… Presumably, protecting 60% of customers has somehow become the industry benchmark for success."*

As it became evident you cannot only focus on preventing attacks from the known malwares and need to be able to protect from new and unknown malwares created every day, new signature-less solutions focusing on behavioral analysis and algorithmic approach started to emerge. This is exactly what CRWD (and some others) did to shake up the reactive legacy security solutions and started to take market share from the legacy vendors.

Moreover, in an on-premise IT environment, there used to be a fence or firewall separating safe data, applications, and users from anything beyond the perimeter but with the rise of cloud, especially in the post-pandemic world, workforce has become extremely mobile which also rendered many of the legacy on-prem IT security solutions much less reliable. These legacy perimeter-based solutions tend to follow "trust but verify" approach which implies once you are verified while entering the system, you are essentially trusted within the system from then on. So all you have to figure out is how to fool the system once.

The unfortunate thing is no matter what solutions you are using, the success rate of preventing these malwares is never going to be 100%. As a result, designing "trust but verify" based system is not quite robust. Consequently, there has been a new approach to address this challenge: Zero Trust approach which does not rely on "trust but verify" but requires users to be authenticated, authorized, and validated before granted access and maintaining access. In fact, last month President Biden has announced an executive order on improving the cybersecurity of the US which insisted on moving to Zero Trust architecture.

As I kept reading to understand the state of cybersecurity, it was difficult not to conclude that companies are awfully underprepared to deal with cybersecurity challenges, and I could not help but have a sinking feeling that practically nobody is quite immune (big or small). For example, two

years ago, one researcher basically proved he could hack the two-factor authentication system and take over any Instagram account he wishes. If almost a trillion-dollar market cap mega-tech company was living under such vulnerability, I shudder to imagine the reality for the rest. As I was listening to this podcast, it became clear even iOS or Android are not quite airtight either.

With the rise of Ransomware-as-a-Service (RaaS), the economic incentives to attack companies are quite compelling as evidenced by the most recent Coveware report: *"the average ransom payment increased 43 percent from $154,108 in Q4 2020 to $220,000 in Q1 2021, and the median payment in Q1 2021 increased from $49,450 to $78,398, a 58 percent increase."*

Thanks to bitcoin or crypto coins in general, RaaS has become quite a scalable business model and considering how many companies have poor security infrastructure, it is perhaps not a difficult job either for many hackers out there. There are too many high-profile attacks that have happened in recent times to list here and yet, there are hardly any indications that these attacks are going to decline anytime soon. Noah Smith went a step further and wondered whether preventing these attacks is ever going to be possible:

"cybersecurity people will make lots of changes and shore up vulnerabilities. But hacking is a very bespoke thing; each security breach is special and unique. It's not clear whether there can ever be any system that makes critical infrastructure and information durably, reliably secure from cyberattacks."

One optimistic theory about the recent increased frequency of cyberattacks is as legacy and more fragile security solutions are being superseded and more robust solutions are taking market share, hackers feel a sense of urgency to milk as much as possible before stricter and more robust regulations take into effect. Given the frequency of current ransomware attacks, it is becoming abundantly clear that the world of atoms and bits are not quite separate anymore.

To summarize, I want to make four broad conclusions in this section: a) more companies will experience cyberattack, b) alarming number of companies are woefully unprepared to prevent security breaches, c) with the rise of smartphones and IoTs, the number of endpoints will accelerate and a cloud native security solution is likely to be more apt for most companies, and d) legacy security vendors are lagging in protecting the IT infrastructure and yet still have majority of market share which they are likely to continue to cede to new players. I will leave more materials in the recommended reading section which may help quench your further exploration to understand the cybersecurity space a little better.

All four conclusions are significant tailwinds for companies such as CRWD and other cybersecurity players. Let me get into the business model of CRWD.

Section 2: CrowdStrike Business Model

CrowdStrike's ambition is to build the Security Cloud platform in the cybersecurity industry following the footsteps of Salesforce (CRM cloud), Workday (HRM cloud), and ServiceNow (IT service management cloud) in their respective industries.

The founding story goes like this: George Kurtz, one of the co-founders of CRWD and then CTO of McAfee, was on a plane and observed his fellow passenger waiting for 15 minutes as McAfee was scanning the laptop for viruses. Mr. Kurtz thought it was unacceptable and there got to be a

better way to secure our laptops or network. On a Saturday morning in 2011, Kurtz made a 25-slide deck to pitch the idea of CRWD to Warburg Pincus. He received $25 mn seed money i.e. $1 mn/slide and later lamented that he should have made more slides. Jokes aside, Kurtz teamed up with Dmitri Alperovitch (then VP of Threat Research at McAfee) and Gregg Marston to launch CRWD. Alperovitch became the CTO and Marston was CFO when CRWD started, but Alperovitch left the company early last year to launch a nonprofit named Silverado which primarily focuses on cybersecurity in a geopolitical context. The other cofounder Marston retired in 2015, but the details on his departure/current whereabouts seems surprisingly thin on the internet.

The founders made a big and bold bet which turned out to be farsighted and successful one. CRWD was the first native cloud security solution. While this sounds like an ordinary bet given today's reality, it was certainly not clear that building an endpoint security solution entirely on cloud is going to be a masterstroke. CRWD launched cloud-native endpoint security platform: Falcon. Falcon has two other characteristics that helped it stand out from other players: a lightweight agent, and threat graph.

On each endpoint, a single lightweight agent (~35 MB) is installed for local detection and prevention capabilities that can collect and stream high fidelity data to Falcon platform for real-time decision making. Falcon's threat graph, on the other hand, processes, correlates, and analyzes the data in cloud using AI and behavioral pattern-matching approaches. Since the threat graph looks for correlation across entire dataset, it can detect threats and stop security breaches which on-premise legacy security solutions find hard to replicate.

Why is a single lightweight agent important? Falcon platform has multiple modules (discussed shortly) that a customer can choose depending on their security requirements. Adding multiple agents on the endpoint reduces endpoint performance and increases management effort. If you use one CRWD module, you can easily sign up for any other module for 15-day trial on your own. Since all modules are integrated to this single agent, you don't need to install multiple agents for each different security solutions and the sales process can happen seamlessly without any active interactions with a salesperson from CRWD if you are already in the Falcon platform. This becomes particularly important once you realize an average enterprise has ~75 security solutions and as per a recent report by Gartner, almost half of the enterprises surveyed indicated that they want to consolidate their security vendors in the next 2-3 years.

Even though CRWD had just 10 modules when it came to IPO two years ago, it currently has 19 different security modules (shown below) and it appears that CRWD's plan is to keep integrating additional modules to its Falcon platform organically or via acquisitions (e.g. recent Humio acquisition). Of these modules, Prevent, Discover, OverWatch, and Insight are the most penetrated among CRWD's ~10,000 subscriber base. While these four modules grew at a similar rate last year compared to overall customer base, there are three modules management identified as "hypergrowth" modules: Falcon Complete, Falcon X, and Falcon Spotlight. You can also click any of the link below to explore each of the module further.

CRWD Modules
Falcon X (Threat intelligence)
Falcon OverWatch (Managed threat hunting)
Falcon Insight (Endpoint Detection and Response)
Falcon Prevent (Next Generation Anti Virus)

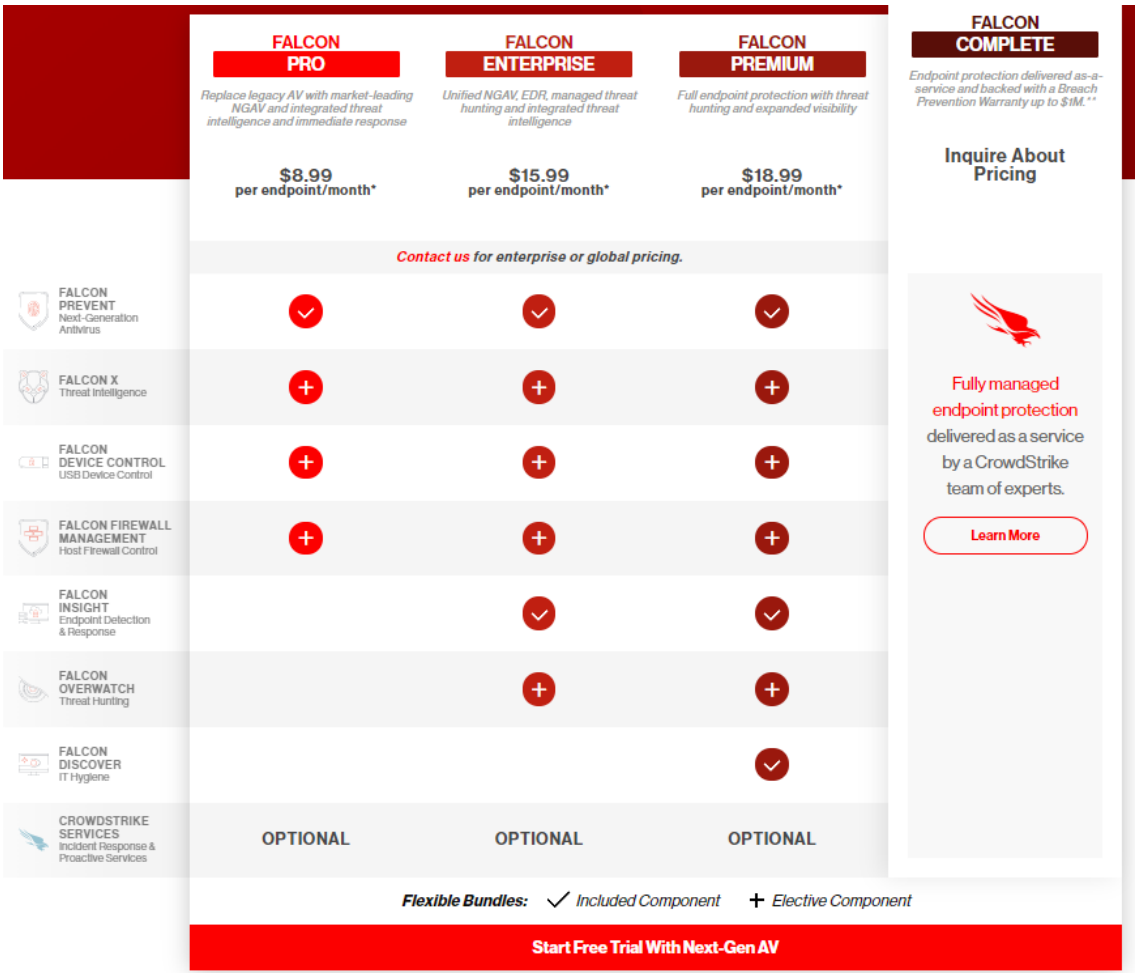
Falcon Discover (Network Security Monitoring)
Falcon Search Engine (Search across all malware collected by the platform)
Falcon Spotlight (Vulnerability Management)
Falcon sandbox (Analyze malware in a safe environment)
Falcon Complete (managed detection and response)
Falcon Device control (Endpoint Device Control & USB Security)
Falcon CWP (Cloud workload protection)
Falcon Discover for cloud environments
Falcon Firewall Management (manage host based firewall policies - on the device)
Falcon Identity Threat Detection (prevent golden ticket attacks)
Falcon Zero Trust (additional insight into identities and account directories)
Falcon Horizon (Cloud Security Posture Management)
Falcon forensics (incident response tool for identifying relevant security event data)
Falcon X Recon (additionally threat intelligence from digital sources)
Humio (log management/Extended Detection and Response or XDR)

A gradually increasing number of modules has been one of the core drivers of success for CRWD. As you can see below, as number of modules in Falcon platform increased over the last five years, percentage of customers who adopted four or more modules increased from literally ZERO percentage in FY'17 to 64% in 1Q'22. In fact, 50% subscribers have adopted >5 modules, and 27% did >6 modules. This has consequently enhanced the net revenue retention and since the additional module comes with very, very high gross margin, CRWD's gross margin more than doubled from 35.5% in FY'17 to 73.7% in FY'21. As subscribers continue to adopt more and more modules, margins may continue to incrementally improve. In the 1Q'22 call, CFO mentioned more and more customers are adopting multiple modules right out of the gate as adoption of multiple modules also makes sense from customers' perspective because of the ease of deployment as well as rationalization of total cost of ownership.

FY	**2017**	**2018**	**2019**	**2020**	**2021**	**1Q'22**
% of subscribers with >4 modules	0.0%	30.0%	47.0%	55.0%	63.0%	64.0%
Net revenue retention	104%	119%	147%	124%	125%	120+%
GAAP Gross Margin	35.5%	54.1%	65.1%	70.6%	73.7%	74.1%

In terms of pricing, Falcon platform has four alternatives: Falcon Pro, Falcon Enterprise, Falcon Premium, and Falcon Complete. In the April analyst call, CRWD outlined how it has been rapidly growing in both premium and small accounts. To put this in context, let me quote CRWD's CFO here: *"**some of the legacy vendors in this space had hundreds of thousands of enterprise customers.** The key to our rapidly expanding customer base is that we are winning customers of all sizes. From a one-person shop all the way to the largest companies in the world, we can sell into any vertical, geography or any level of technical sophistication. Essentially, we can sell to almost anyone."*

ARR	2017	2021	CAGR	ARR mix
> $1 mn	10	176	105%	~40%
Between $100k and $1 mn	151	1,569	80%	~40%
<$100k	286	8,151	131%	~20%
Overall # of subscribers	447	9,896	117%	$1.05 Bn (FY'21)



Because of this module adoption dynamic, landing a new customer/subscriber is of paramount importance in CRWD's business model. It is essentially a "land and expand" model in which you acquire a new customer and then continue to gradually deepen penetration in the customer's security wallet at a pretty high margin. What makes this business even more attractive is security solutions are generally very sticky. Although gross retention rate was reported to be 98% in FY'21, a typical subscription deal with enterprise customer lasts 1-3 years. Given the contractual terms, not all customers are up for renewals every year and hence, assuming the average length of deal is two years, the underlying retention rate is slightly lower (see this thread). In any case, even after this adjustment, retention data is mighty impressive.

FY	2018	2019	2020	2021
Gross retention rate	93.0%	96.0%	97.0%	98.0%
Underlying retention rate	86.0%	92.0%	94.0%	96.0%

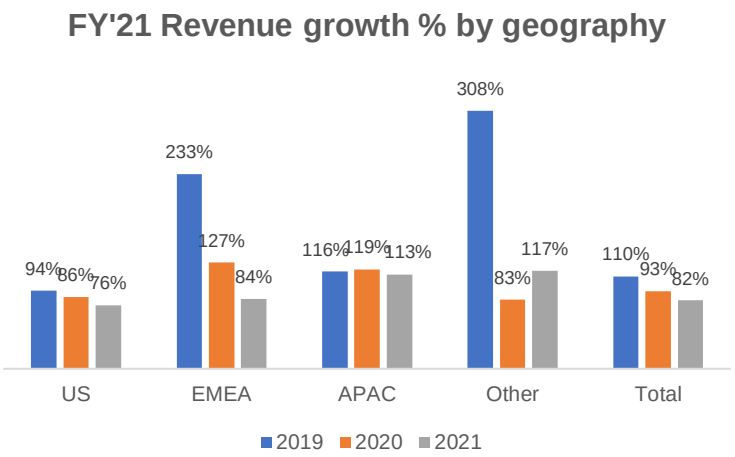
Apart from subscription, CRWD also has Professional Services segment which include services such as incident response/forensic services, technical assessment and strategic advisory services, and training. As CRWD ramped up its subscriber base, services mix in the overall revenue has declined precipitously over the years. Although services is a lower gross margin business (~36% vs ~77% in subscription), it is essentially an incredible customer acquisition tool.

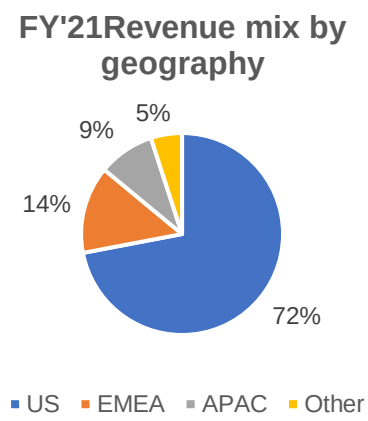
In normal times, companies want to negotiate hard with CRWD given the number of competitive offerings (discussed later). Even if CRWD has the best tech, it is conceivable that many companies don't quite appreciate or even understand the value of having the best of the breed endpoint security, especially since CRWD may not be the cheapest solution out there. It's like having a high-deductible health insurance plan which feels great to have when you are healthy since you pay low premium, but when something bad happens to you, you wish you didn't go for such high-deductible plans. Similarly, when a security breach happens, the customer stops trusting the original vendor and, in many cases, go to CRWD for professional services to figure out what went wrong.

As you can imagine, companies feel very vulnerable during such a time and if CRWD gets the job done, not only does CRWD earn the trust of the customer but also become much more willing to pay premium for such a trusted endpoint security vendor. The fact that services is just a great customer acquisition tool becomes clear from CRWD's 10-k, *"After experiencing the benefits of our platform firsthand, many of our incident response customers become subscription customers. Among organizations who first became a customer after February 1, 2019,* ***for each $1.00 spent by those customers on their initial engagement*** *for our incident response or proactive services, as of January 31, 2021,* ***we derived an average of $5.51 in ARR*** *from those subscription contracts."*

Revenue mix	2017	2018	2019	2020	2021
Subscription	71.8%	78.0%	87.8%	90.6%	92.0%
Services	28.2%	22.0%	12.2%	9.4%	8.0%

While CRWD is a global company, 72% of its FY'21 revenue came from the US. As you can see, international growth has consistently outpaced the growth in the US, and management has indicated that in the long-term they expect the revenue mix to be 50-50 between the US and international.





Overall, the business model appears to be highly lucrative: recurring subscription revenues with high retention and expanding dollar retention through more and more modular adoption (i.e. Land & Expand). The services segment is also a great customer acquisition tool that allows further upsell/cross sell in the Falcon platform. Let me discuss the size of the opportunity for CRWD.

Section 3: Sizing up the opportunity

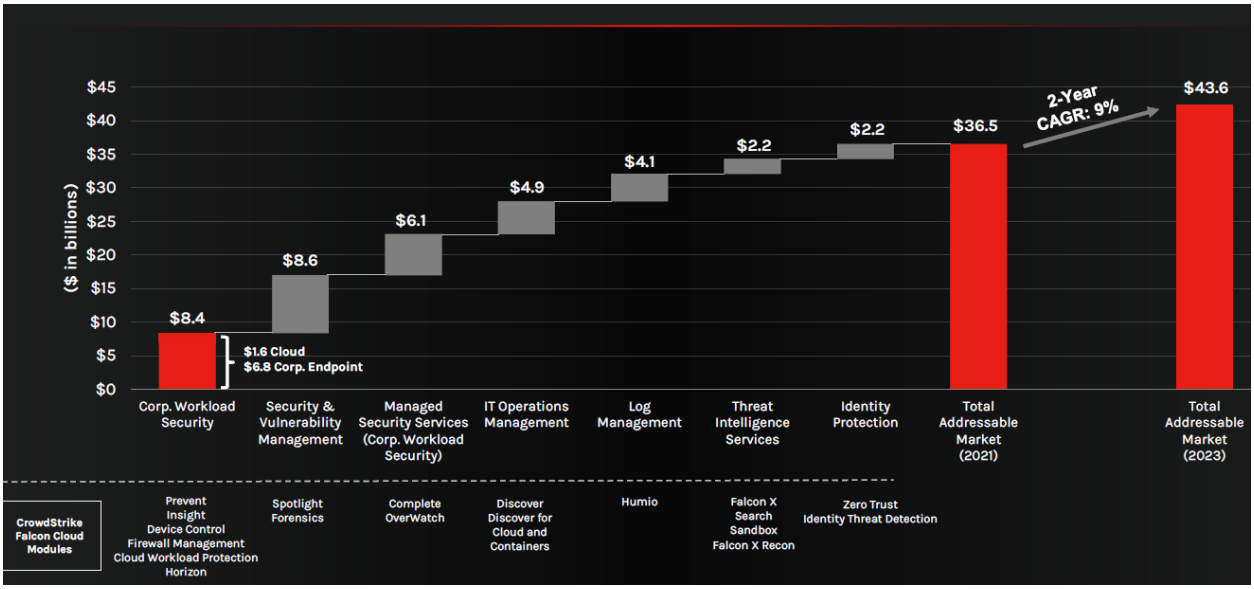
In the April Analyst call, CRWD estimated the Total Addressable Market (TAM) to be $36.5 Bn in 2021 and $43.6 Bn in 2023. CRWD cited these estimates mostly from IDC. While CRWD generates majority of its revenue from endpoint security products today, it is increasingly focusing on cloud workload security. A cloud workload is a distinct work function that you put on a cloud instance, so cloud workload security is basically just protecting these workloads from breaches. If you use public clouds such as AWS, they are responsible for the security ***of*** cloud itself whereas the customer is responsible for implementing security ***in*** the cloud.

CRWD cited IDC to highlight that an organization should spend ~5-10% of its budget on IT security. As IaaS+ PaaS cloud revenue estimates is $217.7 Bn in 2023, it implies $12.4 Bn opportunity for cloud security (assuming 5.7% of IaaS +PaaS expenditure spent on security).

As a generalist, I have to admit that I have found it difficult to assess the reasonableness of these estimates on a segment-by-segment basis. Since CRWD does not disclose revenue by each of these segments mentioned below, it is hard to say how deeply they are penetrated in each security verticals. They do, however, disclose that the four most adopted module are: Prevent, Discover, OverWatch, and Insight, and the next three "hypergrowth" module are Complete, X, and Spotlight.

While reading a recent sell-side initiation, I have come across estimates by Gartner, and Gartner sized endpoint security market and cloud security market to be ~$9 Bn in 2021 and $12 Bn in 2023. Gartner's estimates for cloud security market is ~$1.7 Bn in 2021 and $2.5 Bn in 2023. The Sell-side report mentioned a caveat that this is an early attempt by Gartner to size up cloud security opportunity and it is possible Gartner may revise upward once cloud adoption accelerates further. Understanding the size of the opportunity is sort of important here as you will see in my estimates, CRWD will need to generate ~$10 Bn topline (or ~12x of 2020 revenue) in 2030 to

make sense of the current valuation. Considering this "requirement", it is of paramount importance that CRWD's ambition of being a security platform gets realized over time.



One question that I was wondering was why exactly we didn't have a security platform yet. I was going through an expert call of former sales rep of CRWD and he hinted at the reason:

"If you think about the space, we've grown up into a space where you're very spot on, very much it was a point solution. You buy products. You find out who the leader quadrant is in any respective area. You go buy that product. It became less about the integration from a platform point of view."

In a way, it makes sense to buy best-of-the-breed point solutions when it comes to protecting your IT infrastructure. When you buy a CRM/HRM solutions or software, good enough solutions can work. The "price" for not having the best-of-the-breed point solutions for every little thing is perhaps not too high. But good enough solutions may not simply cut it in security products as the price for good enough solutions can be a security breach which is obviously a non-starter. Therefore, if a company wants to build a security platform, they need to offer best-of-the-breed solutions for everything. Can CRWD pull that off? Let me quote the aforementioned expert:

"It's a tough call to say is it more likely that they can do it. I'm real close to 50/50 on it. I think they've got a good head start from a data point of view, from a security integrity point of view, but there's a lot of companies that are taking data from CrowdStrike, for example, and bringing it into if you could think about firewall review, security, SIEMs, managed service providers, to bring all that data in for the customer's benefit. Endpoint is simply one piece of the data. It's one source of many.

For CrowdStrike to extend the influence, they're going to have to do something they've never done before, which is complete acquisitions, be successful doing that. Can they do that? Can they move beyond their core competency, successfully? You've probably seen many businesses struggle with that. That's a challenge. Everyone wants to grow organically, but you get to a point where you can only grow organically so far."

It does seem CRWD also understands the importance of acquisitions in realizing their broader ambition. They seem to be more active in last few quarters in acquiring companies to bolster their

platform modules. In September 2020, CRWD bought Preempt Security for ~$90 mn which developed real-time access control and threat prevention technology, and in March 2021, they also acquired Humio for $400 mn, a provider of high-performance cloud log management and observability technology. As you can gauge, this is just simply too early to evaluate their deals. If recent pace of deals is any indication, it seems increasingly likely that CRWD will be acquiring more and more companies in the next few years.

There are potential roadblocks from public cloud hyperscalers in the cloud security market as they have their native solutions as well. One big limiting factor is the multi-cloud strategy by many enterprise customers which can tempt those companies to choose CRWD's solutions that can be deployed across multiple clouds. But companies that are exclusive to AWS, Azure, or GCP can potentially just choose the native cloud security solutions offered by the public cloud vendor which is also possibly cheaper.

While asking a question in a recent analyst call, one sell-side analyst hinted at something that makes me think cloud security can possibly be a land grab opportunity and whoever gets there first may end up creating some sort of moat:

"…when you look over to the cloud world and you start talking about workload, runtime protection, I mean, we've clearly got an agent bloat problem on endpoints. But I would think in the cloud server environment, AWS is not going to let more than 1or 2 agents onto their server. And therefore, I would think that, that's even more rarified."

When a company is in a hypergrowth stage as CRWD is currently in, it is understandable that it is hard to fit the whole piece of the puzzle and we may have more questions than answers. At one hand, I can sense a big opportunity that can be extended way beyond the core endpoint security, and on the other hand, it feels the range of potential outcome remains too wide.

Section 4: Competitive Dynamics

Endpoint security is a pretty crowded market and it has been going through bit of a transformation in the last five years. Broadly speaking, endpoint security market can be segmented in five categories: a) Legacy companies (Symantec, McAfee, Trend Micro, Sophos, Eset, Kaspersky), b) Next Generation Companies (CrowdStrike, Carbon Black, Cylance, SentinelOne, Endgame), c) Microsoft which basically deserves to be a category itself, d) Platform Play (Avast, Cisco, FireEye, Palo Alto Networks, Check Point Software), and e) other fringe cybersecurity companies.

As you can see below, legacy companies lost ~33% market share and this market share is primarily being grabbed by Microsoft and Next-generation players. CRWD had ~6% market share in 2019, as per this Gartner report and given its growth acceleration, it will have ~12% market share by the end of 2021.

Vendor	2015	2016	2017	2018	2019
Legacy	78%	79%	67%	53%	46%
Next-Generation	0%	1%	8%	10%	13%
Microsoft	1%	1%	1%	17%	23%
Platform Play	3%	2%	3%	5%	5%
Others	18%	17%	22%	14%	12%

Source: Gartner, Berenberg Capital Markets

Before discussing Next-generation companies, and Microsoft vs CRWD, let me spend a little more time on the legacy vendors.

Symantec, McAfee, and Trend Micro are the three biggest players among the legacy vendors. Symantec had always been focused on selling on-prem perpetual licenses and they only launched their cloud based endpoint security solution in October 2019. Trend Micro also launched cloud offering and rebranded their endpoint security solution as "Apex One" in March 2019. McAfee was a little early than those legacy vendors as they released their cloud-based offering in 2018, but even then, only ~50% of their business is from the cloud offering. They recently sold their enterprise business to Symphony Technology Group, a technology private equity firm, and decided to solely focus on consumer cybersecurity. Overall, it appears they had been caught wrong-footed by the next generation cybersecurity companies and although they have been trying to respond, they are unlikely to protect their market share. By the next 5 years, it is perhaps more likely that the legacy vendors will have <20% market share.

Of the next-generation companies, Carbon Black (acquired by VMware for $2.1 Bn in 2019), Cylance (acquired by BlackBerry for $1.4 Bn), and SentinelOne (S) just filed for IPO. Cylance's revenues were "slightly up" in FY'20 which indicates the integration didn't quite go well considering the hypergrowth CRWD and S were seeing. Before getting acquired, Carbon Black grew its revenue by 30% in 2018, again not quite up to the mark compared to ~110% growth posted by CRWD with similar revenue base in 2018. Although Carbon Black has similar tech, managed threat-hunting service is not available for customers.

SentinelOne (S) is perhaps the closest next-generation endpoint security competitor for CRWD. Founded in 2013 (two years after CRWD), S is raising $100 mn (vs $665 mn in 2019 by CRWD) from its IPO. You can see the comparison of several metrics between CRWD and S when they filed for IPO.

	At IPO	
Indicators	CRWD	S
LTM Revenue	$250 M	$130 M
LTM Revenue Growth	110%	102%
# of customers	2,516	4,700
LTM customer growth	103%	74%
Annual Contract Value (ACV)	$99,294	$27,756
# of modules	10	8
LTM Gross Margin	65.1%	55.8%
Net revenue expansion	147%	119%

S&M as % of revenue	69%	87%
R&D as % of revenue	34%	69%
LTM Operating Margin	-55%	-136%
LTM FCF Margin	-26%	-81%

Although CRWD and S seem largely comparable in revenue growth when they filed for IPO, S appears to be in relatively worse shape in almost every metric out there. The only thing that stood out from the numbers is S has almost ~2x the customers CRWD had when CRWD filed for IPO, but S has ~25% of the ACV compared to CRWD.

Although S' customers include three of the Fortune 10, 37 of the Fortune 500, and 66 of the Global 2000, ACV implies that most of S' customers are small businesses. CRWD raised prices just before going for IPO which helped its net revenue expansion rate, but that seems an unlikely route for S given how intensely competitive the industry has become.

My broader takeaway from reading CRWD and S filings is that their tech is somewhat similar even though both companies love to claim they are superior. S has a separate page on their website explaining how they are better than CRWD, and CRWD CEO also picked on S during their recent earnings call, but all of this is highly likely to be just "marketing" talks.

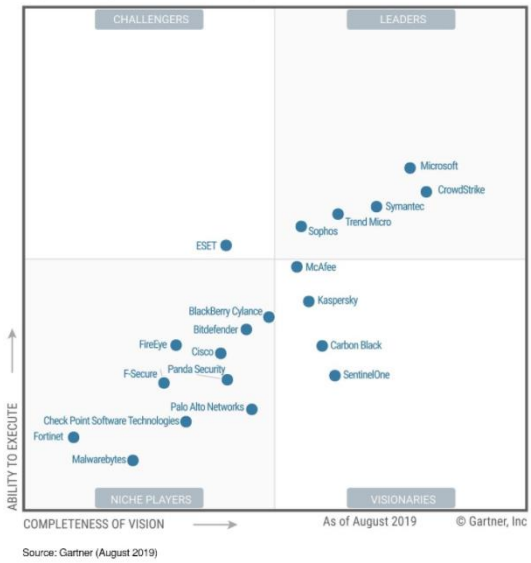
One of the things I noticed is players in this industry have somewhat belligerent tone to competitors, a possible indication of everyone's "insecurity" and the impression I have left with from my readings is tech is not an ongoing moat here. CRWD had a head start and they were decisive in capitalizing that head start, but next-generation companies such as S have similar tech, but by the curse of being late, they may have a hard time to catch up with CRWD's marketing and distribution prowess. It is also possible that they might figure out a few niches (think geography or industry verticals) within the broader cybersecurity and can just manically focus on those niches. As a result, with IPO money S can, at the very least, increase CAC for CRWD going forward.

Even though endpoint security (or cybersecurity) is pretty crowded market, looking at Gartner's Magic Quadrant over the last five years, I found the velocity of change in this space quite dizzying. Two companies (MSFT and CRWD) who were barely there 4/5 years ago (CRWD wasn't even there in 2016) have now become the market leaders with some distance from the rest. It naturally also raises the question whether it is possible for a startup with a better tech to do the same to current incumbents. Gartner's Magic Quadrants are somewhat lagging and powerful indicators at the moment, but it has almost no predictable power 3-5 years down the line. Despite CRWD and MSFT's market leadership, it appears VCs still think the market is far from settled. A LOT of capital is still chasing this market.

Source: Gartner (February 2016)

Source: Gartner (January 2017)

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (August 2019)

Source: Gartner (May 2021)

For example, Deep Instinct just raised $100 mn in their Series D in April, 2021, making their total capital raised to $200 mn. They are backed by the likes of Nvidia, Blackrock, Millennium, Coatue etc. Deep Instinct have a different approach to endpoint security than CRWD. While CRWD follows machine learning approach to protect endpoints, Deep Instinct utilizes deep learning in their security solutions. Let me quote from their website to explain why they think deep learning is preferred over machine learning: *"Machine Learning systems rely on feature engineering which is limited to the knowledge of the security expert who has to handcraft the features for detection. Machine learning-based solutions are still producing low detection rates for new malware and high false-positive rates… The autonomy of the training and prediction stages are enhanced with Deep Learning, so that the algorithm can analyze all the raw data in a file and is not limited by an expert's capabilities. This represents a quantum leap in computer science. For cybersecurity this enables a more advanced level of protection; with higher detection rates of unknown malware, lowest false-positive rates and the ability to detect prior to execution, effectively in zero-time."*

Can CRWD just copy deep learning approach if that is indeed the future? That is a hard question to answer and usually the way these things work, by the time the incumbent realizes they need to drastically tweak their approach to keep up with the tech, it may become too late. Perhaps CRWD will prove to be different, but that is a question CRWD shareholders need to get comfortable with.

If tech is not a sustainable moat and distribution is the probable answer to the moat question, that naturally leads our discussion to perhaps the most important debate: how will CRWD compete against MSFT?

Looking at the market share data and Gartner's Magic Quadrant, it is pretty clear Microsoft has become a behemoth in this industry in almost out of nowhere. MSFT reported $10 Bn revenue from security segment in 2020, growing 40% YoY which makes the growth itself equivalent of 3x CRWD's total ARR in 2020. However, MSFT's security offerings go way beyond just endpoint security and therefore, it is not quite apple-to-apple comparison; nonetheless, it does provide a window of strength of MSFT's hold over enterprise customers.

Ever since Microsoft Exchange Hack became public, there have been questions about how strong their security offerings are which CRWD never fails to mention in their earnings call. I still find it hard to believe that there are too many people out there who will get fired by going with MSFT over CRWD/any other competitor. My broader impression from my readings is it is a question of when, not if, that all cybersecurity firms will experience breach at some point. Ultimately, distribution advantage can tip the favor to MSFT for a lot of enterprise customers. When a former sales rep of CRWD was asked why customers may not choose CRWD over MSFT, this is what he said:

"I'll start with the biggest no-brainer to maybe not go with CrowdStrike. Microsoft is one of the best in the business at selling Enterprise License Agreements (ELA), getting customers who'll sell 365, who'll do a bunch of other stuff. They can land and expand pretty much better than most any other company I've ever seen before. They create these licenses. They continue to try to get sticky with customers in that capacity so customers start to work with Microsoft and the easy answer is, "We've already got Microsoft. Why would we even entertain somebody else like a CrowdStrike?" for example. That would be probably one where I would say it might be harder for CrowdStrike to break in some of those accounts."

One CRWD shareholder I spoke with mentioned to me that he expects more and more enterprise customers to go with CRWD over MSFT because there is hardly any point in buying a cheaper bullet proof vest if it does not do a good job of protecting from an incoming bullet. With the rapid rise of ransomware and more awareness than the past, it is likely that companies may lean to quality over price. However, many C-suites don't quite understand how to evaluate the quality of competing offerings and an MSFT bundle may sound good enough for a lot of enterprise customers. Another quote to explain this dynamic from an expert call:

"Microsoft goes in from the top down, the CIO, CFO, and then they get pushed out of the CSO. In a perfect world for Microsoft customers, they can talk more about what they think that they need their CSOs to do. They can control the narrative from the top down. CrowdStrike is getting to the point where they can start to have more of those conversations, but they still can't do it to the scale that Microsoft can."

If we look beyond endpoint security and assess competition on cloud security (CRWD's next area of focus), there are a few interesting startups on this space as well. Wiz, founded just a year ago and backed by Sequoia, Index Ventures, Insight Partners etc., raised $130 mn and valued at $1.7 Bn. The founder sold his previous company Adallom to MSFT for $320 Mn.

Remember when I mentioned that public cloud vendors may not allow too many agents on their server which can become a moat for CRWD since they already have one? Well, Wiz doesn't require any agent and can support multi-cloud environments.

Then there is also Orca Security which raised $210 Mn in Series C round and backed by the likes of GGV Capital and CapitalG. As discussed earlier, hyperscalers have their own cloud security solution on their servers, but for enterprise customers with multi-cloud strategy may not opt for such solutions. Besides, there have been some concerns about misalignment between public cloud companies and their users as the cost of breach is borne by the end customers and customers don't usually leave from the cloud in drove after a breach is occurred on the cloud which does not give an enormous incentives for cloud vendors to invest in security.

There is a school of thought in investing that moats are over-rated, especially in technology sector. In the fast-paced tech world, it is essentially a Red Queen's race in which you constantly have to run at least at the same pace to keep your position. It is difficult to predict whether the current incumbents will find themselves in the same position 3-5 years down the line.

If there is one conclusion I could derive with confidence, it is that cybersecurity space will see tons of acquisition going forward. There is no way all these companies will be able to scale and survive together. Of course, barring any antitrust concerns, nobody has deeper pockets than MSFT or other big tech companies. Given CRWD's growing revenue and balance sheet size, they may still do well and MSFT's success may not be an existential question for CRWD. Let's figure out now what exactly we need to believe in for CRWD shareholders to generate a decent IRR from current prices.

Section 5: Valuation/model assumptions

If you are reading my deep dive for the first time, I encourage you to read my piece on "approach to valuation". I follow an "expectations investing" or reverse DCF approach and try to figure out what I need to assume to generate a decent IRR from an investment (in this case ~7). Then I glance through the model and ask myself how comfortable I am with these assumptions. As always, I encourage you to download the model and build your own narrative and forecast as you see fit to come to your own conclusion. None of us has the crystal ball to forecast 5-10 years down the line, but it's always helpful to figure out what we need to assume to generate decent return.

Let me discuss the model first, and then I will elaborate on valuation.

Revenue: CRWD grew its revenue at ~75% CAGR in the last 5 years and it is modeled to grow at ~28% CAGR in the next 10 years to ~$10 Bn i.e. ~11.5x revenue of FY'21 revenue of $874 mn.

As mentioned in Section 2, CRWD has two revenue segments: subscriptions (92% of overall revenue), and services (8% of overall revenue).

Within subscription revenues, CRWD segments it in three categories: a) new customers, b) renewal of existing customers, and c) additional endpoints or modules of existing customers.

As the business has scaled, new customers contribution to overall subscription revenue declined from 74% in FY'18 to 33% in FY'21. Similarly, as more and more customers join the Falcon platform, revenue from renewal of existing customers shot up from 14% in FY'18 to 36% in FY'21, and revenue from additional endpoints/modules increased from 12% in FY'18 to 31% in FY'21. With more module adoption, I expect the third bucket to be the dominant revenue contributor in the long-term.

With deeper penetration in the market, I assume CRWD will likely have higher mix of new customers from the ARR <$100k segment. That is why I modeled 2% decline both in revenue per new customer as well as revenue from renewal of existing customer. On the other hand, I assumed increased acquisition activity which will enhance value proposition of the Falcon platform; at the same time, CRWD may also organically add to its existing 19 modules. As more and more customers will choose 5/6 or even more modules, I assume revenue per subscriber from the third bucket will increase at a much faster rate.

Amount in USD Mn, except %	**2017A**	**2018A**	**2019A**	**2020A**	**2021A**	**2022E**	**2023E**	**2024E**	**2025E**	**2026E**	**2027E**	**2028E**	**2029E**	**2030E**	**2031E**
Revenue	53	119	250	481	874	1,371	1,985	2,722	3,554	4,472	5,459	6,485	7,589	8,770	10,023
Growth in absolute USD Mn		66	131	232	393	496	614	737	833	918	987	1,026	1,104	1,180	1,254
Growth		*125.1%*	*110.4%*	*92.7%*	*81.6%*	*56.8%*	*44.8%*	*37.1%*	*30.6%*	*25.8%*	*22.1%*	*18.8%*	*17.0%*	*15.6%*	*14.3%*
Subscription Customers (abs #)	450	1,242	2,516	5,431	9,896	15,446	21,784	28,836	36,544	44,731	53,349	62,334	71,608	81,085	90,671
Growth		*176.0%*	*102.6%*	*115.9%*	*82.2%*	*56.1%*	*41.0%*	*32.4%*	*26.7%*	*22.4%*	*19.3%*	*16.8%*	*14.9%*	*13.2%*	*11.8%*
ARR	59	141	313	600	1,050	1,651	2,392	3,279	4,282	5,388	6,577	7,813	9,144	10,566	12,076
ARR/Subscriber		*113,779*	*124,267*	*110,561*	*106,109*	*106,915*	*109,787*	*113,725*	*117,188*	*120,452*	*123,289*	*125,349*	*127,690*	*130,304*	*133,189*
Revenue to ARR	90%	84%	80%	80%	83%	*83.0%*	*83.0%*	*83.0%*	*83.0%*	*83.0%*	*83.0%*	*83.0%*	*83.0%*	*83.0%*	*83.0%*
Subscription revenues	38	93	219	436	805	1,273	1,858	2,557	3,348	4,224	5,174	6,172	7,245	8,391	9,606
Growth		*144.3%*	*137.0%*	*98.9%*	*84.4%*	*58.2%*	*46.0%*	*37.6%*	*30.9%*	*26.2%*	*22.5%*	*19.3%*	*17.4%*	*15.8%*	*14.5%*
Revenue per subscription		109,418	116,765	109,808	105,000	100,466	99,815	101,020	102,420	103,954	105,515	106,705	108,176	109,901	111,862
Growth			*6.7%*	*-6.0%*	*-4.4%*	*-4.3%*	*-0.6%*	*1.2%*	*1.4%*	*1.5%*	*1.5%*	*1.1%*	*1.4%*	*1.6%*	*1.8%*
ARR per subscription		167	166	151	137	130	128	130	131	133	134	135	137	138	141
DBNER	104%	119%	147%	124%	125%										
New Customer (revenue mix)		74.0%	59.0%	40.0%	33.0%	*24.9%*	*19.1%*	*15.1%*	*12.4%*	*10.2%*	*8.6%*	*7.4%*	*6.3%*	*5.5%*	*4.8%*
Revenue from New Customer		69	129	175	266	317	355	387	414	431	445	455	460	461	456
Growth			*89.0%*	*34.8%*	*52.1%*	*19.4%*	*11.9%*	*9.0%*	*7.1%*	*4.1%*	*3.2%*	*2.2%*	*1.2%*	*0.1%*	*-0.9%*
New Subscriber		852	1,327	3,005	4,556	5,695	6,549	7,335	8,069	8,634	9,152	9,609	9,994	10,294	10,499
Revenue per New Customer		80,436	97,542	58,077	58,282	57,117	55,974	54,855	53,758	52,683	51,629	50,596	49,584	48,593	47,621
Growth			21%	-40%	0%	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*
Renewal of existing customers (rev mix)		14.0%	23.0%	33.0%	36.0%	*37.8%*	*39.7%*	*40.0%*	*39.9%*	*39.4%*	*38.8%*	*38.0%*	*37.1%*	*36.1%*	*35.0%*
Revenue from customer renewal		13	50	144	290	482	737	1,024	1,335	1,666	2,009	2,348	2,688	3,027	3,359
Growth			*289%*	*185%*	*101%*	*66%*	*53%*	*39%*	*30%*	*25%*	*21%*	*17%*	*15%*	*13%*	*11%*
Gross retention rate		93.0%	*96.0%*	*97.0%*	*98.0%*										
Underlying retention rate		86.0%	92.0%	94.0%	96.0%	*97.0%*	*97.0%*	*97.5%*	*98.0%*	*98.5%*	*99.0%*	*99.0%*	*99.0%*	*99.0%*	*99.0%*
Revenue per existing customer		99,068	149,518	215,179	204,820	200,723	196,709	192,775	188,919	185,141	181,438	177,809	174,253	170,768	167,353
Growth			*50.9%*	*43.9%*	*-4.8%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*	*-2.0%*
Additional endpoints or modules (rev mix)		12.0%	18.0%	27.0%	31.0%	37%	41%	45%	48%	50%	53%	55%	57%	58%	60%
Revenue from additional endpoints/modules		11	39	118	249	474	767	1,146	1,599	2,127	2,721	3,370	4,096	4,903	5,791
Growth			*255.5%*	*198.3%*	*111.7%*	*90.1%*	*61.6%*	*49.6%*	*39.5%*	*33.0%*	*27.9%*	*23.8%*	*21.6%*	*19.7%*	*18.1%*
Per subscriber		*13*	*21*	*30*	*33*	37	41	45	49	52	55	58	61	64	67
Growth				*41.1%*	*9.8%*	*15.0%*	*10.0%*	*10.0%*	*8.0%*	*7.0%*	*6.0%*	*5.0%*	*5.0%*	*5.0%*	*5.0%*
% of subs with >4 modules	*0.0%*	*30.0%*	*47.0%*	*55.0%*	*63.0%*										
ARPU (renewal+additional)		99,081	149,539	215,208	204,852	200,761	196,750	192,820	188,968	185,193	181,493	177,867	174,314	170,832	167,420
Professional Services revenue	15	26	30	45	70	98	127	165	206	248	285	313	345	379	417
Growth		*76.3%*	*16.2%*	*48.2%*	*54.7%*	*40.0%*	*30.0%*	*30.0%*	*25.0%*	*20.0%*	*15.0%*	*10.0%*	*10.0%*	*10.0%*	*10.0%*
As % of total revenue	28.2%	22.0%	12.2%	9.4%	8.0%	7.1%	6.4%	6.1%	5.8%	5.5%	5.2%	4.8%	4.5%	4.3%	4.2%

To project the number of subscribers, I have utilized some aspects from the Customer-based Corporate Valuation (CBCV) that I came across the recent Mauboussin paper. You can read my twitter thread on the paper here. For the sake of simplicity, I assumed the entire 450 subscribers were added in FY'17. With some simple retention(or churn) assumption, I built the following table. Given CRWD's consistently high retention, I primarily focused on YoY growth on gross subscriber additions. I defined CAC as Sales & Marketing expenses (excluding SBC) multiplied by % of S&M that is "growth expense" (assumed to be 90% of S&M), and then divide it by gross subscriber

additions. There are two factors that are at play to increase CAC going forward: intensifying competition, and as CRWD moves from early adopters to early majority/late majority in the s-curve, CAC typically increases during these transitions. Ultimately, however, if the tech does not consistently remain topnotch, CRWD may face the "S-curve chasm". As discussed earlier, the velocity of change in this industry makes long-term forecasting not only difficult but also a bit futile since a lot depends on CRWD's ability to maintain the innovator leadership in cybersecurity.

Cohort	Gross additions	Growth	S&M, ex SB	CAC	2017A	2018A	2019A	2020A	2021A	2022E	2023E	2024E	2025E	2026E	2027E	2028E	2029E	2030E	2031E
2017A	450		54		450	390	371	360	356	352	349	345	342	338	335	332	328	325	322
2018A	852	89%	106	$ 111,667		852	818	802	794	786	778	770	763	755	748	740	733	725	718
2019A	1,327	56%	178	$ 120,619			1,327	1,265	1,252	1,240	1,227	1,215	1,203	1,191	1,179	1,167	1,155	1,144	1,132
2020A	3,005	126%	291	$ 87,005				3,005	2,938	2,908	2,879	2,850	2,822	2,794	2,766	2,738	2,711	2,683	2,657
2021A	4,556	52%	452	$ 89,261					4,556	4,465	4,420	4,376	4,332	4,289	4,246	4,204	4,162	4,120	4,079
2022E	5,695	25%	493	$ 77,980						5,695	5,581	5,525	5,470	5,415	5,361	5,308	5,255	5,202	5,150
2023E	6,549	15%	715	$ 98,201							6,549	6,418	6,354	6,291	6,228	6,166	6,104	6,043	5,982
2024E	7,335	12%	925	$ 113,547								7,335	7,189	7,117	7,046	6,975	6,905	6,836	6,768
2025E	8,069	10%	1173	$ 130,832									8,069	7,908	7,828	7,750	7,673	7,596	7,520
2026E	8,634	7%	1431	$ 149,175										8,634	8,461	8,376	8,293	8,210	8,128
2027E	9,152	6%	1692	$ 166,429											9,152	8,969	8,879	8,790	8,702
2028E	9,609	5%	1946	$ 182,218												9,609	9,417	9,323	9,230
2029E	9,994	4%	2277	$ 205,037													9,994	9,794	9,696
2030E	10,294	3%	2631	$ 230,026														10,294	10,088
2031E	10,499	2%	3007	$ 257,759															10,499
Total subscribers					**450**	**1,242**	**2,516**	**5,431**	**9,896**	**15,446**	**21,784**	**28,836**	**36,544**	**44,731**	**53,349**	**62,334**	**71,608**	**81,085**	**90,671**

Cost structure: As discussed earlier, CRWD's gross margin increased materially from ~35% in FY'17 to ~74% in FY'21. While services margin expanded by 10 percentage points, almost all of this massive improvement is due to expansion in subscription margins. CRWD guided long-term gross margins to be ~75-80%+. My long-term gross margins exceeded the high-end of that guide, but if module upsell continues for the entire decade, perhaps ~85% non-GAAP gross margin for subscription is not unrealistic.

However, there is a caveat to this nirvana-like gross margin expansion. One thing I think about a lot is how dependent almost all of these SaaS companies are on public cloud (AWS/ Azure/ GCP). All these SaaS companies tout ~30-50% FCF margins in the terminal state which reminds me of the infamous Bezos quip, "your margin is my opportunity". This used to be grim reaper for many retail companies, and when I think about the dependency on public cloud, and public cloud's oligopoly structure, it is hard not to worry about pricing power public cloud companies may have on current SMID cap SaaS companies. Will Bezos & Co. really allow these SaaS companies enjoy ~40-50% FCF margins when these public clouds are laying out the infrastructure guardrails and spending on capex like crazy.

For context, AWS has spent an estimated $40 Bn capex in the last three years which is ~40% of sales generated by AWS in the last three years. Once these investments are largely done and the world's IT infrastructure mostly migrates to cloud, who is going to stop ~5% price increases every year if they want? Perhaps GCP is the biggest blessing from SaaS companies' perspective since if it were duopoly of AWS and Azure (another App Store?), this could have been potentially even worse competitive dynamics. Even then, I am not quite convinced that in 10 years, all three public cloud companies will not just largely "cooperate" each other, especially if GCP's market share lags AWS and Azure significantly.

If this is the case, perhaps gross margin in subscription segment may not reach ~85% even with increased adoption of modules. Moreover, CRWD highlighted AWS marketplace as one of the important sales channels which cut down sales cycle by ~50%. ARR on AWS marketplace grew 650% in FY'21 to $50 mn (~5% of ARR). I do not know the margin implications of AWS marketplace, but I do think, too much dependence on such sales channel may introduce fragility over the long-term even though it can appear lucrative in short to medium term.

One interesting development I noticed is there have already been some murmurs whether public cloud has too much power and whether it is long-term beneficial for scaled SaaS companies to remain on public cloud (see this piece). However, many of the criticism seems weak (I am a shareholder of AMZN and GOOG, so I can be biased in these inferences).

One investor mentioned to me recently that there is no guarantee that AWS/other public cloud won't be like "Oracle" in 10 years, as in companies will be beholden to their infrastructure and even if service quality fall or price increases gradually, it will be difficult to get out of public cloud which means many of these SaaS companies will not have much leverage in dealing with public clouds.

Amount in USD Mn, except %	2017A	2018A	2019A	2020A	2021A	2022E	2023E	2024E	2025E	2026E	2027E	2028E	2029E	2030E	2031E
Cost of revenue	**34**	**54**	**87**	**142**	**230**	**324**	**452**	**602**	**763**	**931**	**1,100**	**1,261**	**1,426**	**1,592**	**1,807**
As % of revenue	*64.5%*	*45.9%*	*34.9%*	*29.4%*	*26.3%*	*23.6%*	*22.8%*	*22.1%*	*21.5%*	*20.8%*	*20.2%*	*19.4%*	*18.8%*	*18.2%*	*18.0%*
Gross Profit	*19*	*64*	*163*	*340*	*645*	*1,047*	*1,533*	*2,120*	*2,791*	*3,541*	*4,359*	*5,224*	*6,163*	*7,178*	*8,217*
Gross Margin	*35.5%*	*54.1%*	*65.1%*	*70.6%*	*73.7%*	*76.4%*	*77.2%*	*77.9%*	*78.5%*	*79.2%*	*79.8%*	*80.6%*	*81.2%*	*81.8%*	*82.0%*
Non-GAAP Gross Margin	*35.7%*	*54.4%*	*65.4%*	*72.2%*	*75.8%*	*78.5%*	*79.2%*	*79.8%*	*80.4%*	*81.0%*	*81.5%*	*82.2%*	*82.8%*	*83.3%*	*83.4%*
Subscription COGS	24	40	69	112	185	262	373	499	634	777	924	1,068	1,213	1,359	1,551
Cost per subscriber		*47,112*	*36,832*	*28,306*	*24,168*	*20,696*	*20,013*	*19,699*	*19,409*	*19,127*	*18,834*	*18,460*	*18,120*	*17,804*	*18,066*
SBC	0	0	1	5	12	20	29	38	49	59	70	80	91	101	110
As % of subscription revenue	*0.1%*	*0.1%*	*0.3%*	*1.2%*	*1.5%*	*1.6%*	*1.6%*	*1.5%*	*1.5%*	*1.4%*	*1.4%*	*1.3%*	*1.3%*	*1.2%*	*1.2%*
Subscription COGS, excluding SBC	24	40	69	107	174	242	344	460	586	718	854	988	1,123	1,259	1,441
As % of subscription revenue	*64.2%*	*43.0%*	*31.2%*	*24.6%*	*21.6%*	*19.0%*	*18.5%*	*18.0%*	*17.5%*	*17.0%*	*16.5%*	*16.0%*	*15.5%*	*15.0%*	*15.0%*
Services COGS	10	15	18	29	44	62	80	103	129	154	177	194	212	233	255
SBC	0	0	0	2	6	9	11	14	17	20	23	24	26	28	30
As % of Services revenue	*0.3%*	*1.0%*	*0.7%*	*5.5%*	*8.6%*	*9.0%*	*8.8%*	*8.6%*	*8.4%*	*8.2%*	*8.0%*	*7.8%*	*7.6%*	*7.4%*	*7.2%*
Services COGS, excluding SBC	10	14	18	27	38	53	69	89	111	134	154	169	186	205	225
As % of Services revenue	*64.6%*	*54.9%*	*58.6%*	*59.1%*	*54.9%*	*54.0%*	*54.0%*	*54.0%*	*54.0%*	*54.0%*	*54.0%*	*54.0%*	*54.0%*	*54.0%*	*54.0%*

CRWD mentioned in its long-term margins guide that S&M, R&D, and G&A to be 30-35%, 15-20%, and 7-9% of revenues respectively. As you can see below, I have assumed the low end of the range in each of the line items in the long-term. I kept incremental return on marketing at ~3x and assumed scale benefits for R&D and G&A line items.

One of the things I realized while covering CRWD is how comparing some metrics across SaaS companies is problematic. For example, ADSK does not capitalize its sales commissions and therefore, it is expensed immediately. On the other hand, CRWD/ZS/S capitalize sales commissions which is later amortized over a longer period. They call this "Deferred contract acquisition costs" and CRWD mentioned in its 10-k that *"Commissions, including referral fees paid to channel partners, earned upon the initial acquisition of a contract or subsequent upsell are amortized over an estimated period of benefit of four years while commissions earned for renewal contracts are amortized over the contractual term of the renewals."* While I think it is reasonable to capitalize some of these costs, my point is companies that do not capitalize such costs and yet report ~30% operating margins are structurally much better than those who do at least purely from accounting margins perspective. Moreover, capitalizing these costs and amortize over time also tend to inflate FCF margins which I will discuss later.

I do think R&D as % of revenue at 15% may seem too low for an industry that has a lot going on and may need a continuous innovation to stay ahead of the competition. On the flip side of this is I have set aside $500 mn cash/year for acquisitions in each of the next 10 years. As mentioned earlier, I do think this industry will experience a lot of M&A activity going forward and if CRWD wants to be de-facto security platform, I am sure they will have to splurge a little to stay ahead. Perhaps this somewhat compensates the optically low R&D as % of revenue (compared to most SaaS companies out there).

Amount in USD Mn, except %	2017A	2018A	2019A	2020A	2021A	2022E	2023E	2024E	2025E	2026E	2027E	2028E	2029E	2030E	2031E
Sales & Marketing (S&M)	54	104	173	267	401	576	831	1,081	1,370	1,673	1,979	2,276	2,652	3,052	3,473
SBC for S&M	1	1	5	24	51	82	116	155	197	241	287	331	376	421	466
SBC as % of revenue	*1.2%*	*1.2%*	*2.1%*	*5.0%*	*5.8%*	*6.0%*	*5.9%*	*5.7%*	*5.6%*	*5.4%*	*5.3%*	*5.1%*	*5.0%*	*4.8%*	*4.7%*
S&M, ex SBC	54	106	178	291	452	*493*	*715*	*925*	*1,173*	*1,431*	*1,692*	*1,946*	*2,277*	*2,631*	*3,007*
S&M per new subscriber		*111,667*	*120,619*	*87,005*	*89,261*	*77,980*	*98,201*	*113,547*	*130,832*	*149,175*	*166,429*	*182,218*	*205,037*	*230,026*	*257,759*
As % of revenue	*103.1%*	*89.0%*	*71.2%*	*60.3%*	*51.7%*	*36.0%*	*36.0%*	*34.0%*	*33.0%*	*32.0%*	*31.0%*	*30.0%*	*30.0%*	*30.0%*	*30.0%*
Incremental return on marketing		*1.3x*	*1.9x*	*2.5x*	*2.9x*	*2.8x*	*2.4x*	*2.9x*	*2.9x*	*3.0x*	*3.2x*	*3.5x*	*2.9x*	*3.0x*	*3.0x*
R&D	39	59	85	130	215	377	533	700	873	1,046	1,215	1,368	1,514	1,649	1,869
SBC for Product Development	1	3	8	15	40	69	96	128	162	197	232	266	300	333	366
SBC as % of revenue	1.1%	2.9%	3.1%	3.2%	4.6%	*5.0%*	*4.9%*	*4.7%*	*4.6%*	*4.4%*	*4.3%*	*4.1%*	*4.0%*	*3.8%*	*3.7%*
R&D, ex SBC	40	62	92	146	255	*308*	*437*	*572*	*711*	*850*	*983*	*1,102*	*1,214*	*1,315*	*1,504*
R&D per subscriber		73,660	49,157	36,640	33,267	24,339	23,460	22,584	21,746	20,909	20,038	19,060	18,131	17,230	17,507
As % of revenue	*75.3%*	*52.5%*	*37.0%*	*30.2%*	*29.2%*	*22.5%*	*22.0%*	*21.0%*	*20.0%*	*19.0%*	*18.0%*	*17.0%*	*16.0%*	*15.0%*	*15.0%*
General & Administrative (G&A)	16	33	42	89	121	219	315	400	482	555	614	720	831	947	1,067
SBC for G&A	1	7	7	33	41	69	96	128	162	197	232	266	300	333	366
SBC as % of revenue	*1.3%*	*6.1%*	*2.7%*	*6.8%*	*4.7%*	*5.0%*	*4.9%*	*4.7%*	*4.6%*	*4.4%*	*4.3%*	*4.1%*	*4.0%*	*3.8%*	*3.7%*
G&A, ex SBC	*17*	*40*	*49*	*122*	*163*	*151*	*218*	*272*	*320*	*358*	*382*	*454*	*531*	*614*	*702*
G&A per subscriber		*46,961*	*25,991*	*30,697*	*21,214*	*11,899*	*11,730*	*10,754*	*9,786*	*8,804*	*7,792*	*7,848*	*7,932*	*8,041*	*8,170*
As % of revenue	*32.4%*	*33.5%*	*19.5%*	*25.3%*	*18.6%*	*11.0%*	*11.0%*	*10.0%*	*9.0%*	*8.0%*	*7.0%*	*7.0%*	*7.0%*	*7.0%*	*7.0%*

Total SBC as % of revenue is assumed to decline from 17.1% in FY'21 to 13.4% in FY'31. I tried to gauge whether SBC as % of revenue really scales with size. Since CRWD aspires to be CRM/WDAY/NOW, I looked at how their SBC as % of revenue scaled. While NOW has shown some scale benefits, CRM and WDAY did not show any such scale benefit yet. It is too early to say which way CRWD will lean as they scale further.

SBC as % of revenue		
Company	FY'17	FY'21
CRM	9.7%	10.3%
WDAY	23.6%	23.3%
NOW	22.8%	19.3%

Given the upfront cash payment and deferred revenue recognition, FCF margins can be volatile in the short-term for many SaaS/cloud companies. However, over the long-term FCF margins tend to converge to GAAP margins, as shown by this blog. Well, not exactly GAAP margins. Since FCF calculation does not exclude SBC, FCF margins tend to converge with (GAAP EBIT+SBC-Capex)/Revenue. As you can see below, currently there is significant difference between such margin and FCF (-0.7% vs 33.5%). However, this gap doesn't get completely closed over time because of the amortization of sales commissions over time which can inflate FCF margins. As always, I strongly encourage you to download the model and build your own narrative and assumptions that you find reasonable.

Amount in USD Mn, except %	2017A	2018A	2019A	2020A	2021A	2022E	2023E	2024E	2025E	2026E	2027E	2028E	2029E	2030E	2031E
EBIT	(91)	(131)	(137)	(146)	(93)	(125)	(146)	(60)	67	267	551	859	1,166	1,530	1,807
Margin	-171.7%	-110.7%	-54.8%	-30.3%	-10.6%	-9.1%	-7.3%	-2.2%	1.9%	6.0%	10.1%	13.3%	15.4%	17.4%	18.0%
EBIT+SBC	(89)	(119)	(116)	(66)	57	123	203	403	653	982	1,395	1,827	2,258	2,746	3,145
Margin	-167.9%	-100.3%	-46.6%	-13.7%	6.5%	9.0%	10.2%	14.8%	18.4%	22.0%	25.5%	28.2%	29.8%	31.3%	31.4%
EBIT+SBC-Capex	(101)	(149)	(159)	(154)	(7)	41	90	266	479	784	1,160	1,557	1,985	2,430	2,814
Margin	-190.9%	-125.1%	-63.6%	-31.9%	-0.7%	3.0%	4.5%	9.8%	13.5%	17.5%	21.3%	24.0%	26.2%	27.7%	28.1%
Free Cash Flow	(64)	(88)	(66)	12	293	419	524	763	1,050	1,446	1,946	2,476	3,011	3,567	4,014
FCF Margin	*-121.6%*	*-74.3%*	*-26.3%*	*2.6%*	*33.5%*	*30.6%*	*26.4%*	*28.0%*	*29.5%*	*32.3%*	*35.6%*	*38.2%*	*39.7%*	*40.7%*	*40.0%*
SBC as % of FCF	N/A	N/A	N/A	642%	51%	59%	66%	61%	56%	49%	43%	39%	36%	34%	33%

Valuation: To generate ~7% IRR, I had to use 36x terminal FCF multiple. Please note that number of shares outstanding is assumed to increase by ~40% over the next 10 years. While 36x seems optically quite expensive in 2031, if CRWD manages to post the numbers I assumed in my model and we remain in the low interest rate world a decade from now, I wouldn't be surprised if CRWD trades at 40-50x FCF multiple at that time. Please note under my assumptions in the model CRWD will grow its topline by ~15% in 2030-31, so trading at ~2-2.5% FCF yield is probably not

as expensive as it may sound at first glance. At 40-50x FCF multiple in terminal year, CRWD may generate ~8-11% IRR from current price (ceteris paribus).

Items		2021A	2022E	2023E	2024E	2025E	2026E	2027E	2028E	2029E	2030E	2031E
OCF		357	501	637	901	1,224	1,644	2,180	2,746	3,284	3,883	4,345
Capex		(64)	(82)	(113)	(137)	(174)	(198)	(234)	(270)	(273)	(316)	(331)
FCF		**293**	**419**	**524**	**763**	**1,050**	**1,446**	**1,946**	**2,476**	**3,011**	**3,567**	**4,014**
FCF/share		1.3	1.8	2.1	2.9	3.8	5.1	6.7	8.3	9.9	11.5	12.7
Terminal FCF multiple												**36.0x**
Terminal Stock price												**458**
Current price*	**228.6**											
Dividend/share		-	-	-	-	-	-	-	-	-	-	-
Cash flow		(229)	-	-	-	-	-	-	-	-	-	458
IRR	**7.2%**											
#diluted shares outstanding		224	239	254	265	275	284	291	298	303	310	315
**Closing price of June 10, 2021*												

Section 6: Management, incentives and Capital allocation

One of the investors I spoke to recently mentioned his skepticism for CRWD given two of the co-founders already left, especially Dmitri Alperovitch. I don't have a good answer why a 41-year-old co-founder and CTO would want to leave a company which still seems to be on very much "Day 1" mode. There might be many good and innocuous reasons, but one shot at the dark could possibly be the controversy Alperovitch found himself in following CRWD's work on DNC's security breach in 2016.

The aforementioned investor was hesitant about CRWD because he prefers tech CEOs to come from strong product background. I think that's a bit too harsh on George Kurtz, and if anything, I am very, very impressed with Kurtz following my due diligence.

First of all, it is indeed true Kurtz's sales skill and charisma seem to put him in the category where Frank Slootman belongs which sound like a pretty good company to me. Here's what an expert had to say about Kurtz:

"It's crazy. I'll point this out. This is why CrowdStrike's crushing it. It has nothing to do with their product. It has nothing to do with their technology. All of that, anyone could figure out, anyone could design. At the end of the day, it has to do with the CEO. George is a phenomenal CEO at selling."

I would also like to point out before founding CRWD, Kurtz was CTO of McAfee. He, in fact, joined McAfee when he sold Foundstone, a company that he founded, for $90 Mn in 2004. Before Foundstone, he co-wrote a best-selling book named "Hacking Exposed" for network administrators to protect themselves against breaches. What I found particularly interesting about Kurtz is he holds a BS in Accounting from Seton Hall University and also holds a CPA license (currently inactive). He joined PwC after graduation and given his childhood interest in computer and coding, he found himself in the cybersecurity consulting team at PwC. From a very humble family background, Kurtz is certainly an outsider to the tech world and yet was able to disrupt legacy incumbents in less than a decade. I think Kurtz is more than just your charismatic CEO some may be prone to think, and someone who can perhaps more than good enough to compensate for the void there may be following the departures of his co-founders.

There are some cultural aspects that also stood out to me. CRWD had adopted remote work long before the pandemic. It had "remote-first distributed workforce" ideology since the inception of the

company and ~70% of the workforce was working remotely before the pandemic. Along with their bold bet on the cloud, CRWD seemed to be ahead of where the world would be heading which is perhaps music to investors' ears in a high velocity industry like cybersecurity.

From capital allocation perspective, CRWD doesn't seem to follow the typical tech playbook of hoarding cash in balance sheet. In January 2021, CRWD issued $750 Mn Senior Notes with 3% coupon. Given the cash flow profile and possible acquisitions in the next few years, it may be likely that more debt issuances will happen which is probably good news if business remains this good (less share dilution). It's still too early to have conviction about the holistic capital allocation framework.

In terms of incentives, the recent proxy mentions some interesting details about sales commission plan for Colin Black (COO) and Michael Carpenter (President, Global Sales and Operations). CRWD's strategy is more revealing in how Mr. Black's commission is tied to cross-selling, and it's good to see long-term incentives are also factored in sales commissions for Mr. Carpenter.

Mr. Henry

For fiscal 2021, Mr. Henry's target annual commission incentive was $550,000, of which 85% was tied to formulaic product or service goals, including (i) the ACV of cross-sales from service bookings (i.e., net new platform sales cross-sold from a services engagement during the fiscal year), (ii) the ACV of services bookings (i.e., sales of professional services offerings) and (iii) the ACV of new logo sponsor bookings (i.e., new logo subscription bookings closed during the fiscal year sourced directly by Mr. Henry). Target annual quotas were set for each goal, along with a base annual commission rate for bookings up to the target annual quota. The commission rate for bookings in excess of the target annual quota increased based on a sliding-scale of up to 250% of the base commission rate specified for bookings above 110% of the target annual quota. In fiscal 2021, Mr. Henry achieved 222.4% of the cross-sales from service bookings goal, 140.6% of the services bookings goal, and 136.8% of the new logo bookings goal.

The remaining 15% of Mr. Henry's target annual commission incentive was based on achievement of discretionary MBOs, including the participating in speaking engagements and other business events, business development meetings, media interviews and other Company events. During fiscal 2021, Mr. Henry participated in over 65 speaking and media engagements and hosted a number of events, including CXO summits. As a result, Mr. Henry achieved 100% of the MBO component of his fiscal 2021 target commission incentive.

Mr. Carpenter

For fiscal 2021, Mr. Carpenter's target annual commission incentive was $550,000, which was tied to "new platform ACV" bookings (i.e., platform sales to new or existing customers that result in additional incremental ARR from the customer) and services booking goals. Target annual quotas were set for each goal, along with a base annual commission rate for bookings up to the target annual quota. The base commission rate for new platform ACV bookings increased based on a sliding-scale for achievement of the target annual quota at 100% or above. In fiscal 2021 Mr. Carpenter achieved 131.7% of the new platform ACV bookings goal and 145.8% of the services bookings goal.

In addition, in order to promote the creation of long-term, sustainable customer relationships, Mr. Carpenter is also eligible to earn commission incentives based on goals that are tied to longer-term customer contracts. Specifically, Mr. Carpenter is eligible to earn commissions on (i) "New Platform TCV Out Years," which represents the total contract value of a new platform contract sale that the customer committed to beyond the first 12-months of the contact period, (ii) "Renewal ACV," which represents the ACV of a renewal booking that results in the same or less ARR with the same customer, and (iii) "Renewal TCV Out Years," which represents the total contract value of a renewal booking that the customer committed to beyond the first 12-months of the contract.

Under the long-term equity incentive compensation plan, two-third of the compensation is in the form of RSUs (tied to stock price) and one-third is PSUs which was tied to the following revenue growth goal in FY'21 (previous year). CEO George Kurtz owns 7.2% of outstanding shares.

Revenue Growth[1] (%)	Achievement Percentage (%)
< 35%	0%
35% (threshold)	50%
55% (target)	100%
≥ 65% (maximum)	130%

Section 7: Final words

In summary, CRWD is an incredible success so far in an area that will only grow in its significance in the future. The company is led by a charismatic CEO who really know the industry cold. At the same time, copious amount of capital is chasing this industry and given the historical velocity of change, I feel it is still difficult to pick stocks. While valuation is certainly demanding, it is not the primary concern I have. If CRWD becomes the de-facto security platform in 5 years, I think it is much more likely that today's valuation will prove to be not expensive in hindsight. But in the scenario the industry remains hard fought among multiple players, or Microsoft becoming the gold standard for security not necessarily due to their tech, but mostly thanks to their outsized distribution advantage, there can be a possible hard landing for today's shareholders. Of course, there is also a very probable scenario that CRWD's customers themselves may experience a breach which can be duly capitalized by other startups and current players. Considering the flux of capital and competition, I am going to mostly observe CRWD and cybersecurity space from a distance for the next couple of years. I think CRWD can be much easier company to own once some of the current crop of startups fail or get acquired and investors gain some sense of clarity of the long-term competitive dynamics.

Of course, waiting for such clarity will also possibly lower return for future shareholders although I think it is unlikely that CRWD is 15-20% IRR investment in the next 10 years from today's prices even if most things go in their favor. Personally, I am fine with lower return potential with higher predictability (but you may not). I am more than happy with high-single-digit to low-double-digit IRR over the long-term from an investment. Considering the range of potential outcome, some may argue for a smaller weight as a starting point. If I owned at today's price, it would certainly be low weight in my portfolio. But there are many of these tech companies that have wide range of outcomes. I am willing to own a bunch of them in a barbell fashion, but I would still wait to gain a reasonable understanding of this group of stocks and then decide later which ones to include in one side of the barbell. For now, I will just focus on adding to my investing knowledge book.

Portfolio discussion: Last month, I added to Etsy ($169/share) and Amazon ($3,232/share). I wrote a thread on Etsy's acquisition of Depop. Etsy also recently announced to issue $1 Bn convertible debt at 0.25% rate (conversion price is 45% above current prices). Personally, I would rather prefer Etsy to just issue standard bonds that don't lead to share dilution in the future.

On Amazon, I have recently read this very interesting thread on twitter which I highly recommend. As an induvial investor, I am always keen on taking/increasing existing position on a stock when I am reasonably comfortable about the long-term, but the street has somewhat legitimate concerns in the short term. Both Etsy and Amazon somewhat currently fit this description as they both face tough comps in the next few quarters. I am willing and happy to underperform in the next few quarters if it hopefully comes with the reward of long-term outperformance. The current sentiment of e-commerce stocks reminds me of BRK in last July when I doubled my BRK

exposure. Market was perhaps legitimately annoyed at how Buffett handled Covid-19 situation, but that annoyance went a bit too far since in July, BRK was trading at near Covid lows whereas the S&P 500 almost recovered the bear market by that time. Since then, BRK outperformed S&P 500 by ~24 percentage points.

I have sold the Vimeo distribution ($45/share) from IAC spin-off and used half of the proceeds to buyback IAC ($159/share).

I have covered ADSK recent earnings here. I am planning to write a short update on Lululemon sometime next week which I initially covered last November. One subscriber recently let me know that there is a silly (but thankfully non-material) formula mistake on my Etsy model. I will upload the correct and updated model sometime in the next week as well. You will receive the updates via email.

Please note that these are not my recommendation to buy/sell these securities, but just disclosure from my end so that you can assess potential biases that I may have because of my own personal portfolio holdings. Always consider my write-up as my personal investing journal and never forget my objectives, risk tolerance, and constraints may have no resemblance to yours.

Ticker	Avg. Cost	Current Weight*	Unrealized Gain %
BRK.B	197.3	19.9%	44.4%
ETSY	128.7	16.7%	29.9%
FB	224.9	16.4%	47.8%
ADSK	289.9	14.4%	-4.3%
IAC	82.8	10.3%	82.7%
AMZN	2,771.2	8.3%	20.9%
GOOG	1,184.6	4.1%	112.9%
ANGI	11.7	3.5%	22.6%
ISRG	558.6	3.5%	53.8%
ANSS	364.0	2.8%	-7.8%
Cash		0.0%	
Total		100%	32.6%

**Based on prices as of June 10, 2021 (time-weighted YTD: +11.3%)*

I encourage you to subscribe for the annual plan; annual subscribers receive the full schedule of deep dives in 2021. ***In case you are curious, I am likely to cover Roku next month****. Please feel free to encourage your colleagues/acquaintances to subscribe to my work. Your support is deeply appreciated. Thank you so much.*

Recommended reading

1. Forbes piece on George Kurtz:

2. Muji's primer on cybersecurity: Flavor of Security

3. Muji on What is Zero Trust?

4. Podcast discussing the current state of cybersecurity

5. Zeynep's piece: Battlestar Galactica Lessons from Ransomware to the Pandemic

6. Thread on Ransomware-as-a-service

7. Software FCF margins: Who has been over-earning?

8. Jamin Ball on SentinelOne S-1

9. Albert Wang's deep dive on CRWD (Bullish)

Disclaimer: All posts on "MBI Deep Dives" are for informational purposes only. This is not a recommendation to buy or sell securities discussed. Please do your own work before investing your money.