PORTFEL TRADERA

CROWDSTRIKE

Analiza

INDEPENDENTTRADER.PL

Spis treści

Wstęp

Crowdstrike to spółka technologiczna z branży cyberbezpieczeństwa, zajmująca się bezpieczeństwem komputerów, monitorowaniem zagrożeń w sieci, a także szkoleniem personelu. Jest to trzecia co do wielkości firma z tej branży (po Microsofcie i Palo Alto Networks), z kapitalizacją przekraczającą 65 mld USD.

Przedsiębiorstwo zostało założone w 2011 roku przez George'a Kurtza, Dmitrija Alperowicza i Gregga Marstona.

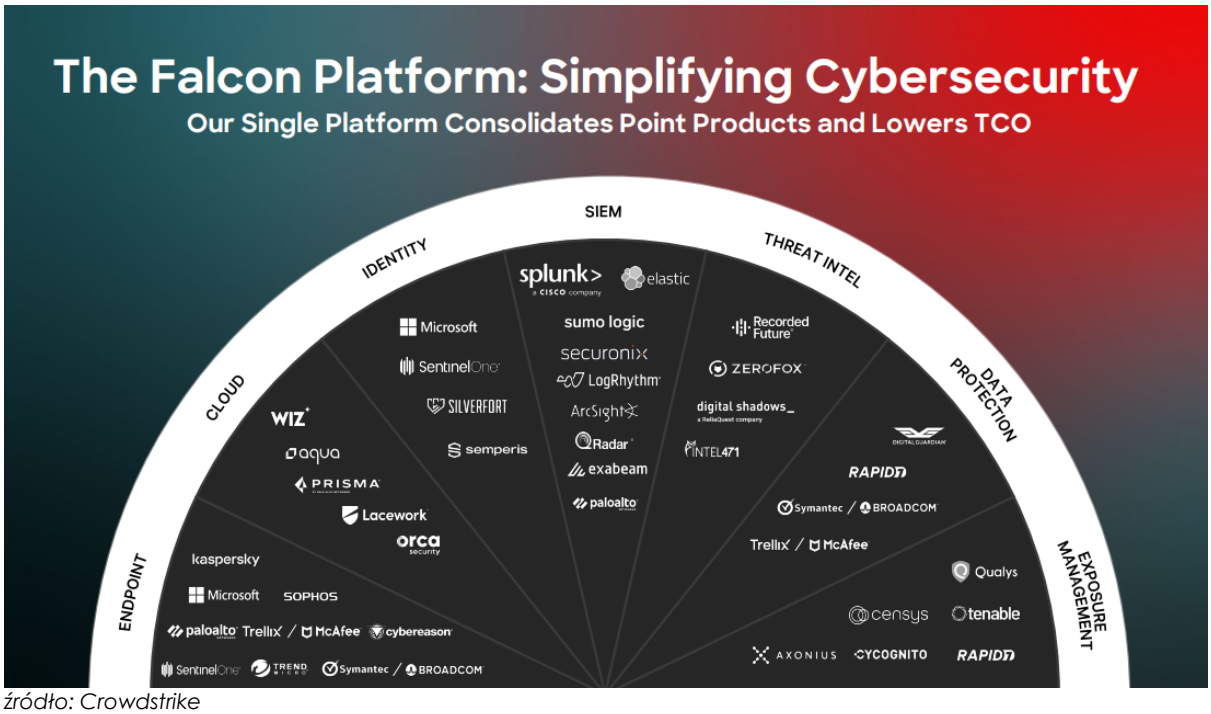
Jest to młoda spółka typu growth, która zadebiutowała na amerykańskiej giełdzie NASDAQ w czerwcu 2019 roku.

Siedziba firmy. Źródło: https://corporateofficeheadquarters.org/

Opis działalności

Przedsiębiorstwo m.in. zajmuje się ochroną urządzeń końcowych - komputerów, laptopów, smartfonów, tabletów etc., słowem wszystkich urządzeń, których używają użytkownicy (zarówno konsumenci jak i pracownicy) do łączenia się z Internetem. Drugim głównym działem jest monitorowaniem zagrożeń sieciowych, tj. gromadzenie i analizowanie informacji o aktualnych i potencjalnych atakach zagrażających bezpieczeństwu firm i ich zasobów. Jest to niezwykle ważny element infrastruktury sieci, ponieważ pozwala na działania wyprzedzające, takie jak aktualizacja oprogramowania czy przeprowadzanie szkoleń personelu. W efekcie maleją zarówno szanse na wystąpienie incydentu (np. kradzieży lub usunięcia danych), jak i potencjalne koszty związane z usuwaniem skutków, jeżeli do takowego dojdzie. Z usług monitorowania zagrożeń sieciowych korzystają zarówno przedsiębiorstwa (przede wszystkim banki) jak i podmioty państwowe (służby, wojsko).

Poniższa grafika przedstawia platformę Falcon – główny produkt Crowdstrike. Na slajdzie zawarto 7 obszarów działania Falcona (kolejno: urządzenia końcowe, chmurę, tożsamość, informacje i zarządzanie wydarzeniami, monitorowanie zagrożeń sieciowych, ochronę danych oraz zarządzanie ekspozycją).



źródło: Crowdstrike

Jest to kompleksowy produkt, który pozwala na zastąpienie rozwiązań bezpieczeństwa wielu innych firm takich jak np. Microsoft, Qualys czy Palo Alto Networks.

Istotnym dla spółki jest przeprowadzanie szkoleń pracowników na temat istniejących zagrożeń i metod zapobiegania i radzenia sobie z nimi. Klientami tych usług są przede wszystkim korporacje kładące duży nacisk na cyberbezpieczeństwo.

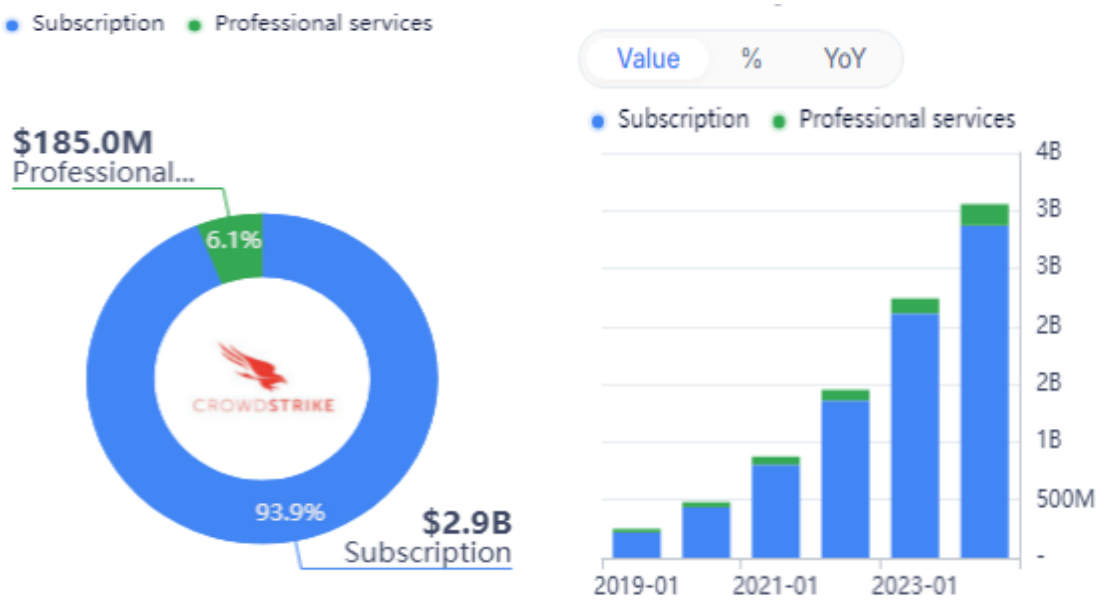
Należy w tym momencie wspomnieć o ostatnim incydencie z 19 lipca 2024 roku, kiedy to wadliwa poprawka została dostarczona na kilka milionów komputerów. Spowodowało to awarie w wielu branżach na świecie, m.in. w handlu, bankowości czy liniach lotniczych, a łączna wartość strat na świecie została wyceniona na około 10 mld USD. Sytuacja została szybko opanowana i nie miała charakteru związanego z rdzeniem działalności firmy, ale z nieprawidłowościami w procesie wdrażania aktualizacji. Samo wydarzenie odbiło się negatywnie na notowaniach spółki (spadek o ponad 14%), ale nie wpłynęło w żadnym stopniu na fundamenty jej funkcjonowania.

W wyniku zaistniałej sytuacji, amerykańskie linie lotnicze Delta Airlines zapowiedziały pozew przeciwko spółce, wyceniając straty spowodowane odwołanymi lotami na 500 mln dolarów. Pod znakiem zapytania stoi też dalsza współpraca Delta Airlines z Crowdstrike i Microsoftem. Crowdstrike pozywają również akcjonariusze, którzy oskarżają spółkę o wprowadzenie w błąd odnośnie bezpieczeństwa procesu testowania oprogramowania, przed jego wprowadzeniem na urządzenia klientów. Kolejnym zagrożeniem jest prawdopodobny pozew zbiorowy od właścicieli małych biznesów, m.in. sklepikarzy, z powodu masowej awarii kas bezobsługowych.

Niewykluczone jest, że działania prawne zostaną podjęte również przeciwko firmie Microsoft, ze względu na bliską współpracę obydwu korporacji.

Rynki i obszary działalności

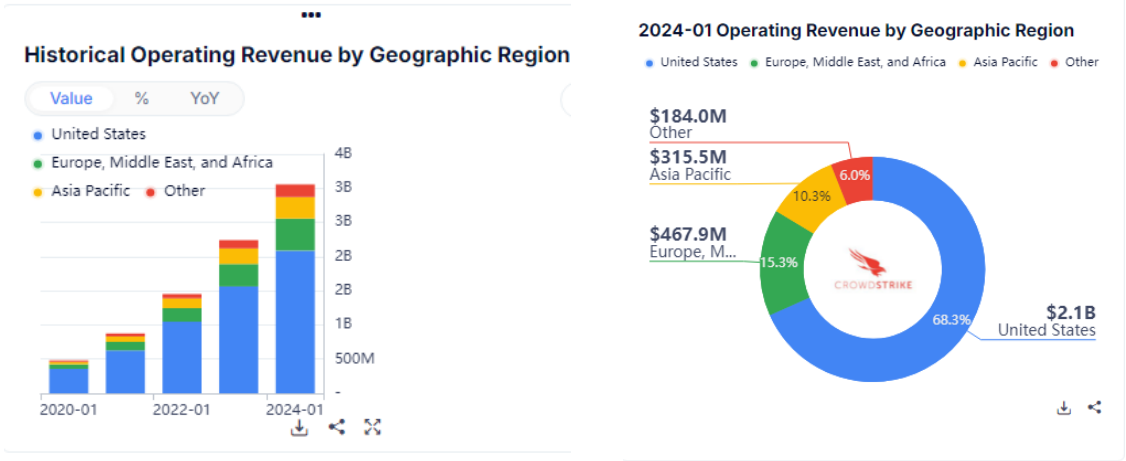
Crowdstrike jest jednym z liderów w branży cyberbezpieczeństwa. Jego flagowy produkt to platforma Falcon. Stanowi ona główne źródło przychodu spółki i działa w modelu subskrypcyjnym, czyli Crowdstrike to firma Software as a Service (SaaS) o czym szerzej pisaliśmy w raporcie o spółkach SaaS. W przypadku tego przedsiębiorstwa od wielu lat zdecydowana większość przychodów (ponad 90%) pochodzi z subskrypcji.



Podział przychodów spółki obecnie i historycznie. Źródło: gurufocus.com

Do produktów spółki należą również rozwiązania polegające na szkoleniu zespołów w reagowaniu, zapobieganiu i zwalczaniu skutków potencjalnych ataków, a także koordynacji zespołów IT. Oprócz tego Crowdstrike bada najnowsze trendy w swojej dziedzinie, stale rozwijając wiedzę i narzędzia. Firma posiada szerokie portfolio klientów, przede wszystkim w Stanach Zjednoczonych i Europie. Są to m.in. stany Arizona, Oklahoma i Wyoming, miasta Las Vegas i Phoenix, największe światowe korporacje, jak Intel, Henkel, Mars, NetApp, Deutsche Telekom (T-Mobile), biura podróży TUI, zespół Formuły 1 Mercedes-AMG Petronas, a także szereg firm z sektora finansowego, przemysłowego i ochrony zdrowia.

Przychody spółki pochodzą z całego świata co przedstawiają poniższe grafiki.



Geograficzny podział przychodów spółki. Źródło: gurufocus.com

Największy udział mają Stany Zjednoczone generujące prawie 70% przychodu spółki. W przypadku tak newralgicznej branży konieczne jest wzięcie pod uwagę geopolityki. Przedsiębiorstwa z państw starających się konkurować z USA nie będą korzystać z usług Crowdstrike. Można zatem zakładać, że struktura przychodów spółki nie zostanie zdywersyfikowana o przedsiębiorstwa chociażby z Chin lub Rosji.

Perspektywy branży cyberbezpieczeństwa

Sektor usług IT stale rośnie, zarówno poprzez jego popularyzację na nowych rynkach jak i coraz większy ich zakres. Mowa tu o takich rozwiązaniach jak e-commerce, płatności internetowe, czy usługi publiczne (w Polsce od wielu lat funkcjonuje Profil Zaufany czy Platforma ePUAP). Nie można także pominąć także rozwoju sztucznej inteligencji (AI), która zwiększa swoje możliwości przede wszystkim dzięki ogromnym zbiorom danych (big data). Wartość danych, które mogą paść ofiarą cyberataku, jak i potencjalne szkody wywołane wpadnięciem ich w niepowołane ręce stale rosną. Mowa tu nie tylko o atakach hackerskich indywidualnych osób, ale również o działalności w charakterze terrorystycznym, wywiadowczym lub wojennym. Już od wielu lat armie na całym świecie wzbogacają się o specjalne oddziały żołnierzy-informatyków, którzy specjalizują się w działaniach zarówno ofensywnych, jak i obronnych.

Bez aktualizowanej na bieżąco ochrony, firmy i organizacje byłyby bezbronne. Aby w pełni zrozumieć powagę sytuacji, należy wyobrazić sobie co czeka podmiot, który zaniedba temat cyberbezpieczeństwa. Wypłynięcie tajemnic przedsiębiorstwa może prowadzić do utraty jego konkurencyjności, utrata

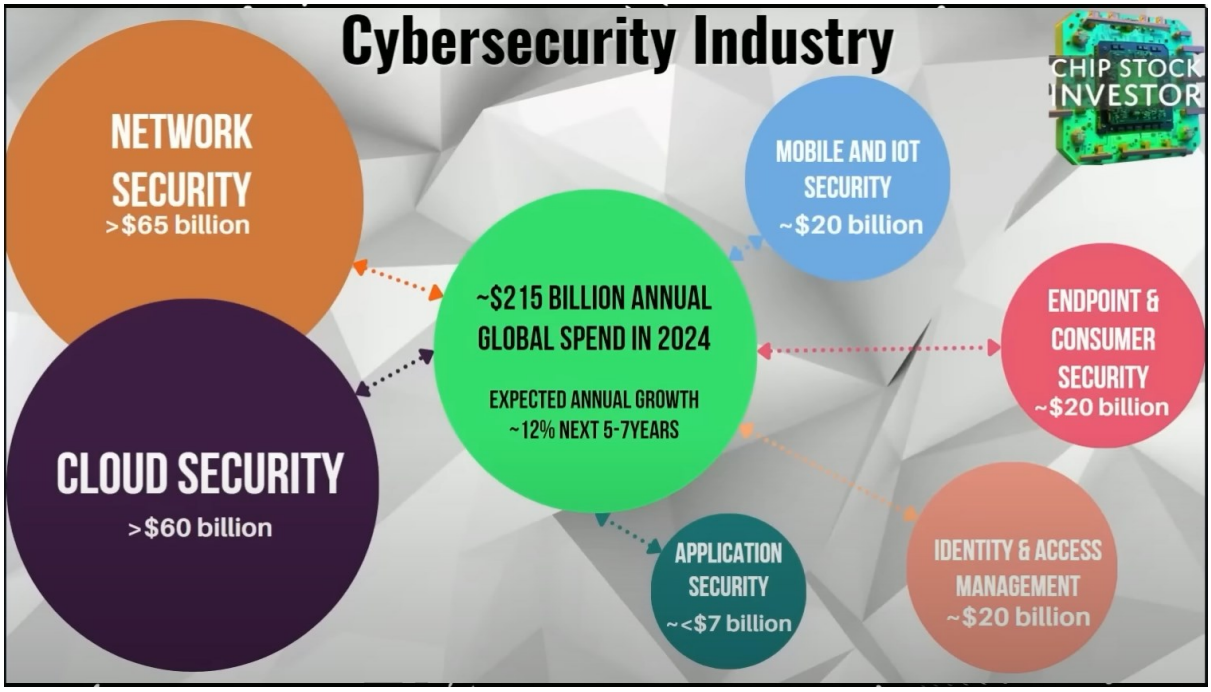
danych użytkowników oznacza milionowe kary ze strony organów państwa, a wyrządzone szkody mogą prowadzić do pozwów od osób i firm trzecich. Najważniejsza jest jednak przede wszystkim utrata zaufania konsumentów, partnerów biznesowych, inwestorów i akcjonariuszy, coś czego odbudowa może zająć długie lata.

W przypadku ataków na państwa, skutki mogą być jeszcze bardziej bolesne. Wyciek danych na temat infrastruktury militarnej mógłby poważnie uszczuplić potencjał obronny. W dzisiejszych czasach grupa zdolnych hackerów jest w stanie wyrządzić szkody porównywalne, a nawet większe od konwencjonalnych działań zbrojnych, przy dużo mniejszym zaangażowaniu sił i środków. Atak na państwo może również sparaliżować kluczowe usługi, takie jak energetyka czy system bankowy, a straty dla gospodarki, w zależności od skutków, mogą kosztować setki miliardów.

Podsumowując, cyberbezpieczeństwo to obecnie jedna z kluczowych dla całego świata branż bez której nie są w stanie funkcjonować istotne sektory, takie jak opieka zdrowotna, finanse czy transport. Ma zatem przed sobą perspektywiczną przyszłość.

Szacuje się, że w 2024 roku na cyberbezpieczeństwo zostanie wydane ponad 200 mld dolarów. Wartość ta ma rosnąć przez kolejne 5-7 lat o 12% z roku na rok. Na poszczególne rodzaje zabezpieczeń zostanie wydane:

- sieć - 65 mld dolarów,
- chmura - 60 mld dolarów,
- urządzenia mobilne i internet rzeczy - 20 mld dolarów,
- urządzenia końcowe i użytkownicy prywatni - 20 mld dolarów,
- ochrona danych - 20 mld dolarów,
- aplikacje - 7 mld dolarów.



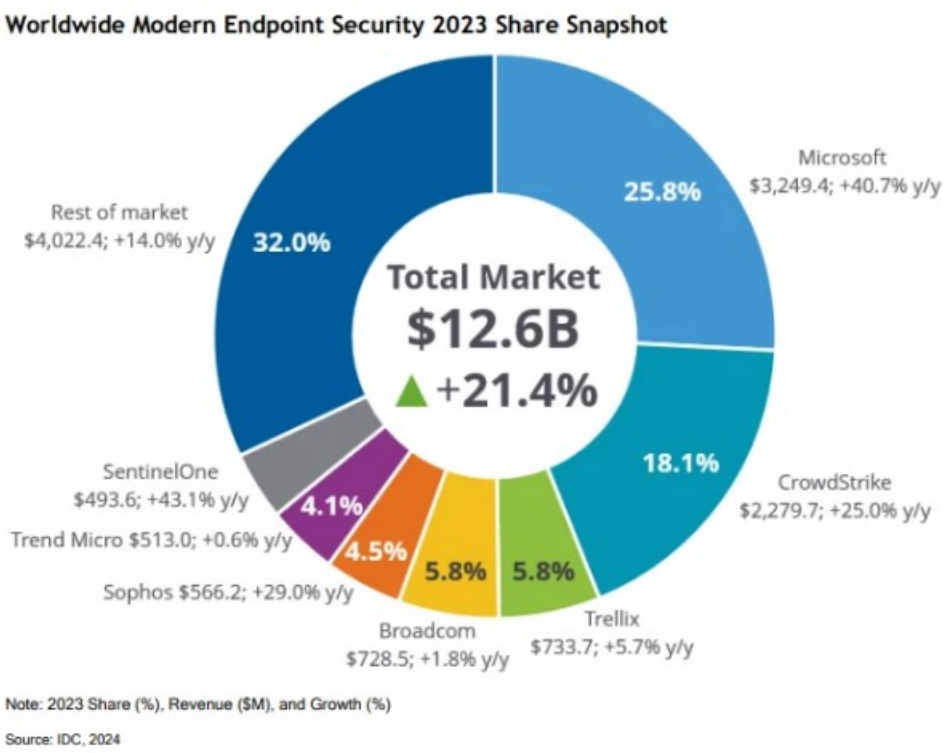
Rynek cybersecurity z podziałem na poszczególne segmenty. Źródło: youtube

Nadchodząca rewolucja komputerów kwantowych całkowicie przemodeluje rynek IT, a w szczególności cyberbezpieczeństwa. Komputer kwantowy będzie w stanie przełamać konwencjonalne zabezpieczenia, takie jak szyfrowanie danych, w czasie kilkudziesięciokrotnie krótszym niż współczesne superkomputery. Duże spółki, a do takich należy Crowdstrike, będą w stanie sfinansować badania w tym zakresie i mogą w przeciągu kilku najbliższych dekad całkowicie wyeliminować mniejszą konkurencję z rynku.

Plany rozwoju

Jednym z najnowszych produktów spółki jest Charlotte AI, będący cyfrowym asystentem dla zespołów bezpieczeństwa IT, przyspieszającym i automatyzującym wiele czynności. Może on m.in. przeszukiwać na bieżąco sieć pod kątem zagrożeń czy wykonywać wewnętrzne audyty bezpieczeństwa, np. poprzez weryfikację haseł użytkowników.

Spółka planuje przede wszystkim dalej rozwijać swój sztandarowy produkt, platformę Falcon i umacniać swoją pozycję w branży cyberbezpieczeństwa. W przeciągu ostatnich 4 lat udział spółki w branży ochrony użytkowników końcowych zwiększył się o prawie 130%, z 7,9% w 2019 roku do 18,1% w 2023 roku. Poniższa grafika przedstawia jaką część tego rynku posiadają poszczególne przedsiębiorstwa.



Podział rynku *bezpieczeństwa urządzeń końcowych. Źródło: IDC*

Warto zanotować, że firma ma już za sobą początkowy etap wzrostu i po raz pierwszy w historii odnotowała zysk netto w 2023 roku.

CRWD

CROWDSTRIKE

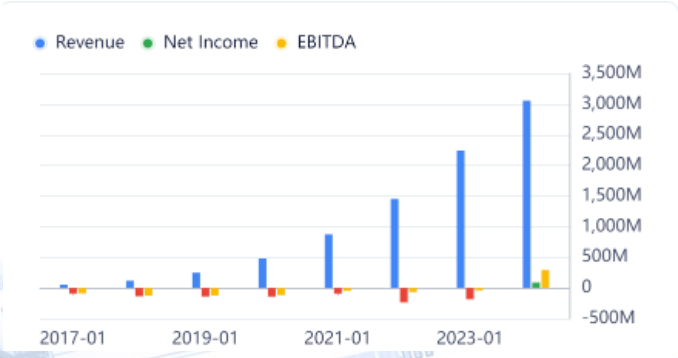
Crowdstrike to trzecia co do wielkości firma zajmująca się cyberbezpieczeństwem na świecie i lider branży endpoint security.

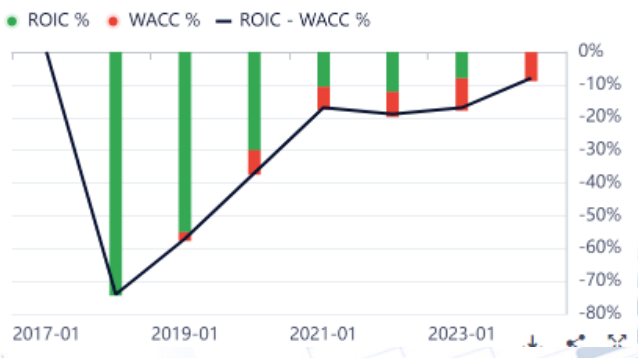
Podstawowe informacje:

Giełda	Nasdaq – USA
Kapitalizacja	65 mld USD
Sektor	Technologia
Ekspozycja na	Cyberbezpieczeństwo
Siedziba	Austin, USA

Wskaźniki:

P/E	379	🔴
Forward P/E	71	🔴
P/S	17.4	🔴
Marża brutto	75%	🟢
Wsk. Altmana	9.22	🟢
Debt to equity	28%	🟡
Progn. wzrost zysku 3-5y	20%	🟢
ROIC-WACC	- 8.67%	🔴



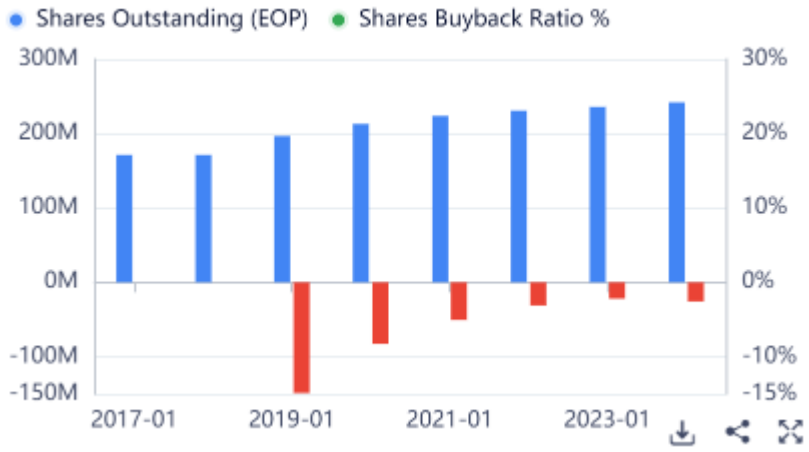


Zalety

- Przedsiębiorstwo z roku na rok zwiększa swoje przychody.
- Spółka działa w jednej z najbardziej perspektywicznych branż na świecie i jako jeden z liderów ma duże szanse na jej zdominowanie – podobnie jak rynek reklam został zdominowany przez Google i Facebooka.
- Bardzo wysoka marża brutto na poziomie 75%. Dzięki niej spółka posiada duży margines bezpieczeństwa na wypadek recesji.
- Cyberbezpieczeństwo jest jednym z podstawowych wydatków firm. Nawet w złym otoczeniu gospodarczym przedsiębiorstwa będą przeznaczać środki na ochronę. Dzięki temu przychody Crowdstrike są stosunkowo odporne na recesje.
- Crowdstrike posiada ponad 4 razy więcej gotówki niż długu. Jest w bardzo dobrej kondycji finansowej (wskaźnik Altmana powyżej 9) i może pozwolić sobie na przejmowanie mniejszych przedsiębiorstw działających w tej samej branży.
- Model działania SaaS jest wysoce skalowalny i pozwala na powtarzalne uzyskiwanie przychodów przez Crowdstrike. Z perspektywy przedsiębiorstwa jest to najlepsza forma zarabiania ze względu na cyklicznie powtarzające się przychody.

Wady

- Przedsiębiorstwo finansuje pensje pracowników dając im opcje na akcje co prowadzi do rozwadniania akcjonariuszy w tempie około 2,6% rocznie (czerwone słupki, prawa skala). Nie jest to jednak znaczna wartość jak na tak zmienną spółkę i co ważne spowalnia od 2019 roku.



źródło: gurufocus

- Crowdstrike jest trudną do wycenienia firmą. Inwestor poszukujący wartości bez większego zastanowienia odrzuci ją ze względu na wskaźnik P/E wynoszący ponad 300. W przypadku tej spółki należy skupić się na jej przewagach konkurencyjnych. Dodatkowo na wysoką wycenę wpływa możliwość konsolidacji branży cyberbezpieczeństwa, w obrębie 2-3 przedsiębiorstw podobnie jak miało to miejsce w przeszłości z innymi internetowymi rozwiązaniami.
- Problemy prawne i medialna nagonka po aktualizacji bezpieczeństwa z lipca 2024 roku.

Podsumowanie

Crowdstrike jest jedną z najważniejszych spółek z branży cyberbezpieczeństwa. Wyróżnia się kompleksowością ochrony i dzięki atrakcyjnej formie promocji platformy Falcon może w przystępny sposób prowadzić tzw. upselling. Zjawisko to polega na oferowaniu przez firmy SaaS lepszych, ale droższych programów. Na przykład zamiast ochrony samych urządzeń końcowych, Crowdstrike może zaoferować szeroką gamę rozwiązań z obszaru cyberbezpieczeństwa dbających o całe przedsiębiorstwo klienta, za odpowiednio większą cenę. Obecnie Crowdstrike oferuje posiadaczom poszczególnych planów ochrony korzystanie z pełnego pakietu do czasu wygaśnięcia ich umów z konkurencją. W ten sposób pozwala klientom na przetestowanie ich rozwiązań. Takie posunięcie pokazuje, że Crowdstrike jest firmą świadomą wyższości swojego produktu nad konkurencją.

Ostatnie spadki akcji z 400 dolarów jest uzasadniony ze względu na wiele pozwów z powodu wadliwej aktualizacji z 19 lipca 2024 roku. W tym przypadku diabeł tkwi w szczegółach i zasady korzystania z rozwiązań Crowdstrike mocno ograniczają potencjalne odszkodowania. W zależności od kontraktu możliwe kary umowne za wadliwą aktualizacje będą kosztować1 – 9 mln dolarów. Kwoty tego rzędu są znacznie mniejsze niż straty Delta Airlines szacowane na 500 mln.

Jeśli jednak sędziowie zdecydują się na znaczne zwiększenie kar dla przedsiębiorstwa niż te wynikające z umów zawartych z klientami, wpłynie to negatywnie na kurs akcji. Podsumowując, wiele zależy od tego jak prawnicy Crowdstrike poradzą sobie z zawieraniem ugód oraz w bataliach sądowych. Należy tutaj zaznaczyć, że anglosaski system prawny jest znacznie bardziej skomplikowany od kontynentalnego. Przez to znacznie więcej zależy od

umiejętności prawników niż od litery prawa w porównaniu do polskiego systemu sądownictwa.

Autorzy: Arkadiusz Kopeć, Karol Natonik

Prezentowane informacje mają charakter wyłącznie informacyjny i edukacyjny oraz nie uwzględniają indywidualnych potrzeb i sytuacji konkretnego Inwestora, w związku z czym nie stanowią rekomendacji wydawanej w ramach usługi doradztwa inwestycyjnego w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi ani też porady inwestycyjnej, w rozumieniu Rozporządzenia PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE.

Informacje nie mają na celu promowania oraz zachęcania do nabycia wskazanych w nich instrumentów finansowych, ani nie stanowią wystarczającej podstawy do podjęcia decyzji o nabyciu instrumentów finansowych, a ewentualne decyzje inwestycyjne podejmowane przez Inwestorów na własny rachunek na podstawie tych informacji powinny zostać poprzedzone indywidualną analizą i oceną ryzyka inwestycyjnego.

Wszelkie decyzje inwestycyjne są podejmowane przez inwestora indywidualnie, na własny rachunek i odpowiedzialność. Autor informuje jedynie o aktywach finansowych, na które inwestor może, lecz nie musi zwrócić uwagi w zakresie własnego niezależnego procesu decyzyjnego. Przed zawarciem jakiejkolwiek z transakcji, każdy klient powinien indywidualnie określić jej potencjalne ryzyko, możliwe korzyści oraz straty z nią związane, jak również jej charakter, konsekwencje prawne, podatkowe i księgowe. Autor nie zataja żadnych informacji, które posiada, a których brak może spowodować szkody w mieniu inwestora.

Karol Natonik oraz osoby fizyczne, osoby prawne i inne podmioty z nim powiązane, w tym w ramach stosunku kontroli, nie mają żadnych powiązań, w tym umownych, ani konfliktów interesów z emitentami instrumentów, których dotyczą przesłane informacje, oraz nie występują żadne okoliczności mogące mieć potencjalnie negatywny wpływ na obiektywność przedstawianych informacji o emitentach.