Corero Network Security

Debt free with growing margins - we upgrade

27th March 2024

For FY23, Corero delivered double digit annualised recurring revenue ('ARR') growth; we see this momentum continuing into FY24E and have upgraded our forecasts accordingly. The retirement of all debt, including an inter-company loan, leaves the balance sheet ungeared and clean of FX movements which made reported margins historically volatile. We see normalised EBITDA margins of 10%+ going forward and potentially rising further. The growth in revenues leaves the stock trading on a forward rating of only 1.8x EV/Sales and we see fair value at 14p price/share.

ARR up more than revenues. Group revenues rose 11% YoY to $22.3m, while exit ARR grew 17% YoY to $16.9m. Most of this revenue growth came from the US (+17% YoY) reflecting both the focus and vicinity of the sales and marketing team. Renewals are running at a very healthy rate of 98%. EBITDA (adjusted for the inter-company loan) rose +32% YoY to $2.2m, implying a 9.8% adj. EBITDA margin. The inter-company loan has now been repaid which will stabilise the reported margin in the Income Statement going forward.

Recurring revenue growth. The drivers for the ARR growth include the Protection-as-a-Service sales (+15% YoY) and Support revenues (+20%). These two service lines recur over multiple periods, termed 'Over Time' revenues when combined and now form over 63% of total revenues (+360bp YoY). Licence sales were flat YoY at $8.2m reflecting the focus on selling 'Over Time' contracts.

New partnerships. New partnerships have been announced with Akamai and TechEnabler over the last two quarters. These announcements portray a channel strategy necessary to move the ex-US revenue base, which was flat last year, into the same growth trajectory as domestic US revenues. We believe more partnerships across multiple territories are in negotiation.

Upgrade. We factor new items such as the full year effect of the $1m TechEnabler contract, strongly performing ARR growth, a greater proportion of software sales and higher gross margins (to 90%) into our forecasts. This leads us to upgrade our FY24E revenue forecast by 3% to $25.3m and EBITDA by 25% to $2.5m. We introduce new FY25E forecasts which factor in continued momentum and 16% YoY growth in EBITDA to $2.9m. Our longer-term view is that the business model and revenue mix should be capable, over time, of delivering an EBITDA margin closer to mid-teens levels.

Debt free. Corero is debt free and has over $5m of net cash on the balance sheet, leaving it self-sustaining on a cash flow basis. Corero has a strong product roadmap with a new 400Gb product being released later this year to help drive sales to new customers. While we don't break-out an ARR forecast, **the stock is trading on a historic EV/ARR rating of 3.0x and by inference is much lower in our forecast periods. This stock has both defensive and growth qualities which should support a higher rating going forward and we reiterate our fair value of 14p price/share.**

Forecasts & Ratios

Y/E Dec, $'m	2020A	2021A	2022A	2023A	2024E	2025E
Group revenue	16.9	20.9	20.1	22.3	25.3	28.6
EBITDA	-1.4	3.3	2.6	1.8	2.5	2.9
PBT	-4.0	1.4	0.4	-0.2	0.6	1.0
Adjusted EPS (p)	-0.8	0.3	0.1	0.0	0.1	0.2
EV/Sales (x)	3.0	2.4	2.5	2.3	2.0	1.8
EV/Ebitda (x)	nm	15.2	19.3	28.8	20.0	17.2

Source: Company Accounts, Equity Development estimates

Company Data

EPIC	CNS
Price (last close)	9.25p
52 weeks Hi/Lo	10.5p/5.75p
Market cap	£47.1m
ED Fair Value / share	14.0p

Share Price, p

Source: ADVFN

Description

Corero Network Security provides DDoS protection solutions, specialising in automatic detection and protection with network visibility, analytics and reporting tools. .

Simon Strong (Analyst)
0207 065 2690
simon.strong@equitydevelopment.co.uk

Hannah Crowe
0207 065 2692
hannah@equitydevelopment.co.uk

Overview

Corero Network Solutions (LON: CNS) is a specialist cyber software business listed in London on AIM. The majority of its revenues are derived from the Americas (71% in FY23A) with the US market being its dominant territory. The Corero product set, named SmartWall One™, prevents against a specific type of cyber security threat called a Distributed Denial of Service (DDoS) attack. These attacks can arise in core networks, in cloud-based environments, network edges or at application levels. Corero provides a pre-emptive solution to counter such attacks in real-time, together with a reporting and analytics functionality to ensure continuing network availability.

Threat landscape

Cyber-security and DDoS threats are not a static risk. These attacks are intensifying every year, year on year, as evidenced by Cloudflare, the security and performance company, in its recent Q4 2023 report. It observes:

- a 117% YoY increase in network-layer DDoS attacks, and overall increased DDoS activity targeting retail, shipment and public relations websites during and around Black Friday and the holiday season.
- DDoS attack traffic, targeting Taiwan, registered 3,370% growth compared to the previous year amidst the upcoming general election and reported tensions with China.
- The percentage of DDoS attack traffic targeting Israeli websites grew by 27% QoQ, and the percentage of DDoS attack traffic targeting Palestinian websites grew by 1,126% QoQ as the military conflict between Israel and Hamas intensified.
- a 618-fold YoY surge in DDoS attack traffic targeting Environmental Services websites coinciding with the 28th UN COP28 Conference.

Hyper-volumetric HTTP DDoS attacks

The size and sophistication of DDoS attacks is also increasing. Particularly complex attacks around HTTP/2 vulnerabilities have been exploited, leading to the largest attack ever witnessed at 201 million requests per second, 8x larger than the previous record.

Geopolitical risk

In our view, it is no coincidence that attacks of this scale and magnitude are intensifying. The build-up of geopolitical tensions globally is not only manifesting itself in kinetic warfare but also in the cyber-sphere. It is developed nations that have been most targeted, with the countries most attacked in Q4 being:

- Singapore,
- United States,
- Canada,
- Taiwan.

Origins of attacks

China generally has been the largest source of HTTP DDoS attack traffic to date, however the US is reported to be the largest source in 2023. It is not disclosed whether state or non-state actors are responsible for attack traffic from the US. China and the US combined account for 25% of all DDoS traffic. Other country origins of attacks include Brazil, Germany, Indonesia and Argentina which account for another 25%.

Channel strategy

Corero has recently signed partnership agreements with:

- Akamai (Oct-23): this agreement will see Corero's SmartWall One™ product sold globally alongside Akamai's traffic inspection and custom mitigation controls to stop DDoS attacks.
- TechEnabler (Dec-23): this agreement will see this Brazilian network solutions provider sell Corero's SmartWall One™ product alongside its third-party network observability platforms across Latin America.

Channel partner research site Canalys estimates that 91% of total cyber security expenditure comes through channel partners, meaning that accessing this growth market via third parties is critical. The strategy to actively pursue and expand the number of partnerships aims to increase Corero's exposure to overseas markets. In FY23A, revenues outside the US and UK represented less than 20% of total sales:

Y/E Dec, $'m Geographic exposure	2022A	2023A
United States	13.5	15.9
United Kingdom	2.3	2.1
Rest of World	4.3	4.4
Total revenues	20.1	22.3

Source: Company Accounts

Overseas markets are a growth opportunity for Corero and we assess how nascent these markets are as follows:

Asia

The Asia-Pacific region saw a 38% increase YoY in DDoS attacks in 2023, with Singapore the largest target according to TechWire Asia. South East Asia experienced the strongest DDoS attack which reached 1.4Tbit per second and lasted 7 minutes with the telecommunications industry seeing the majority (31%) of all attacks. It notes a shift to multi-vector attacks and more complex attack strategies where combined DDoS and non-DDoS elements are used simultaneously. StormWall states that the rise in DDoS attacks correlates with Russian companies increasingly moving into the APAC region. The current sanctions facing Russia has meant that it is forging new partnerships with countries like China, Hong Kong, India, and North Korea, states that have amicable relations with Russia. Market research body IDC is forecasting that Asia-Pacific security spending grew 17% in 2023 to counter these challenges.

Europe

Europe is a developed market for cyber-security expenditure, but warfare and geopolitics are fuelling DDoS attacks. A European Union Agency for Cybersecurity report on the DDoS attack threat landscape found that 66% of DoS attacks are politically motivated and are acts of retaliation triggered by political decisions. Government infrastructure is the preferred target by threat actors, with the government administration sector receiving 46% of attacks. 50% of incidents globally were found to be related to the Russian-Ukrainian war. Furthermore, it notes that the reporting of DDoS attacks has not reached maturity to enable the real extent and impact of such attacks to be fully comprehended. Infosecurity is reporting that 69% of IT leaders are expecting an increase in cyber-security budgets in 2024 of between 10 and 100%.

Latin America

Brazil is a heavily targeted country for DDoS attacks. In H1 2023, Brazil faced 42% of all attacks on the continent according to NetScout. Brazil is heavily targeted, we believe, because of its size and increasing penetration of internet access. Fixed/mobile broadband penetration has recently reached 81% and 86% respectively according to the country's statistics institute, IBGE, and 80% of the population used the internet on a daily basis in 2022, in line with the global average. A recent report from Akamai found that network infrastructure overhead (Layer 3) and transport layer (Layer 4) attacks reached an all-time high, being 50% higher than in 2021. Nearly 30% of all attacks are reported as being on a 'massive' or 'horizontal' scale because they target multiple IPs simultaneously. The Instituto Analisi Relazioni Internazionali (IARI), a geopolitical risk organisation, has found many deficiencies in the cyber-security Latin American cyber security market. It reports little investment, training or awareness of the major issues and that only seven of the thirty-two countries surveyed have a critical infrastructure plan.

Middle East and Africa

It has been common in markets like Europe and Eastern Asia for organisations to prioritise cybersecurity only after they reach a certain size. Internet usage however in Africa has doubled over the last ten years, with around 600 million internet users across the continent. The digitisation of Africa has opened up the threat landscape to malign actors. Kenya recently witnessed a DDoS attack on the country's e-Citizen platform, leaving 5,000 government services unavailable on its portal. *Anonymous Sudan* claimed responsibility and there are claims that it has Russian backing. We believe Africa has been a materially under-invested region for cyber-security to date. However, industry research body Gartner estimates cybersecurity spending in the Middle East and Africa to amount to $7.7bn by 2026 in light of recent attacks, growing at a compound rate of c8%, with security software accounting for 41% of the total. IDC actively highlights digitisation strategies and cloud migration shifts as reasons why the threat landscape is enlarging.

Addressable market – large and growing

Canalys estimates market compound growth rate in the value of the cybersecurity market to be 12% globally. Corero has identified a direct total addressable market for its products of $2bn per annum. On our FY25E revenue forecast, this equates to a market share of only 1.5% leaving plenty of headroom for expansion.

Growth strategy

Corero has an established sales and marketing presence in the US and UK but there is a significant opportunity to commercially exploit growing demand in developing markets for DDoS protection. Reaching these markets directly requires either scale or the establishment of partnerships to extend reach. We believe there are more partnership agreements being pursued by Corero to extend its reach further. With successful execution, Corero has the ability to:

- increase its market share,
- benefit from a double digit growth rate in its underlying market,
- add incremental new customers while maintaining its existing base with a 98% renewals rate,
- participate in existing customer expansion as their data volumes and networks grow and more network protection points are required.

With Corero projected to generate free cash flow this year of £1.7m and have net cash on the balance sheet of over £6.8m by the year end, the business is self-funding. Management has shown aptitude in being able to balance double digit revenue growth and maintain a profitable, positive free cash flow model. The stock is trading on 2.0x EV/Sales in FY24E versus the UK software sector trading on c3.0x. This level of discount to the peer group supports our continued 14p fair value per share assessment.

REVENUE ANALYSIS

Y/E Dec, $k	2019A	2020A	2021A	2022A	2023A	2024E	2025E
SmartWall One™ software and appliances	3,738	8,446	10,337	8,107	8,186	9,005	9,906
% sales	38.5	50.0	49.5	40.3	36.6	35.6	34.6
SmartWall One™ maintenance, services & 'as-a-service'	5,926	8,431	10,558	12,014	14,163	16,287	18,729
% sales	61.0	50.0	50.5	59.7	63.4	64.4	65.4
Legacy maintenance and support services	50	0	0	0	0	0	1
% sales	0.5	0.0	0.0	0.0	0.0	0.0	0.0
Total revenue	9,714	16,877	20,895	20,121	22,349	25,292	28,636

Source: Company Accounts, Equity Development estimates

INCOME STATEMENT

Y/E Dec, $k	2019A	2020A	2021A	2022A	2023A	2024E	2025E
Consolidated Revenue	9,714	16,877	20,895	20,121	22,349	25,292	28,636
Growth yoy	-	73.7%	23.8%	-3.7%	11.1%	13.2%	13.2%
Cost of sales	-1,842	-3,832	-3,112	-2,576	-2,164	-2,529	-2,864
Gross profit	7,872	13,045	17,783	17,545	20,185	22,763	25,772
Gross margin (%)	81.0	77.3	85.1	87.2	90.3	90.0	90.0
R&D	-1,423	-1,562	-1,546	-1,743	-1,920	-2,000	-2,000
Operating expenses	-9,609	-12,911	-12,904	-13,183	-16,508	-18,234	-20,837
EBITDA	-3,160	-1,428	3,333	2,619	1,757	2,529	2,935
EBITDA margin (%)	-32.5	-8.5	16.0	13.0	7.9	10.0	10.3
Depreciation (ex.DPaaS)	-515	-633	-697	-579	-539	-575	-575
Amortisation of intangibles	-2,526	-1,684	-1,495	-1,364	-1,234	-1,400	-1,400
EBIT	-6,201	-3,745	1,141	676	-16	554	960
Other income	0	0	637	0	0	0	0
Net interest	-360	-285	-405	-272	-137	0	0
Profit before tax	-6,561	-4,030	1,373	404	-153	554	960
Tax charge	0	246	149	150	-17	0	0
Profit after tax	-6,561	-3,784	1,522	554	-170	554	960
Basic EPS (p)	-1.6	-0.8	0.3	0.1	0.0	0.1	0.2
Average shares (m)	406.57	494.85	494.85	495.90	495.90	495.90	495.90

Source: Company Accounts, Equity Development estimates

CASH FLOW							
Y/E Dec, $k	**2019 A**	**2020 A**	**2021 A**	**2022 A**	**2023 A**	**2024 E**	**2025 E**
EBIT	-6,201	-3,745	1,141	676	-16	554	960
Depreciation	515	633	697	579	539	575	575
Amortisation of acquired intangibles	13	6	5	2	2	0	0
Amortisation of capitalised development	2,638	1,933	1,872	1,732	1,504	1,732	1,732
Working capital	2,219	5,710	-1,601	-5,254	1,296	680	0
Share based payments	265	359	522	386	230	425	425
Other including exceptional costs	0	0	0	0	30	0	0
Operating Cash Flow	-551	4,896	2,636	-1,879	3,585	3,966	3,692
Net Interest	-281	-190	-237	-151	-34	0	0
Tax	0	246	149	150	-17	0	0
Cash flow pre-capex and investment	-832	4,952	2,548	-1,880	3,534	3,966	3,692
Investment in intangible assets	-6	-8	0	0	0	0	0
Capitalised development expenditure	-1,360	-1,410	-1,754	-1,704	-1,823	-1,750	-1,750
Net capex	-579	-1,015	-421	-420	-813	-500	-500
Acquisitions/disposals	0	0	0	0	0	0	0
Financing/other	3,028	-686	842	-1,240	-1,277	0	0
Dividends	0	0	0	0	0	0	0
FX & other	44	-14	-154	-311	-107	0	0
Net Cash Flow	295	1,819	1,061	-5,555	-486	1,716	1,442
Closing Net Cash/(Debt) pre-IFRS 16	5,384	7,662	8,424	4,438	5,160	6,876	8,318

Source: Company Accounts, Equity Development estimates

BALANCE SHEET							
Y/E Dec, $k	**2019A**	**2020A**	**2021A**	**2022A**	**2023A**	**2024E**	**2025E**
Fixed Assets							
Goodwill	8,991	8,991	8,991	8,991	8,991	8,991	8,991
Acquired intangible assets	7	9	4	2	0	0	0
Capitalised development expenditure	5,169	4,646	4,528	4,500	4,820	5,170	5,520
Tangible assets	652	1,099	796	604	633	558	483
Leased right of use assets	357	237	145	62	309	250	200
Trade & other receivables	307	694	859	0	0	0	0
Total Fixed Assets	15,483	15,676	15,323	14,159	14,753	14,969	15,194
Current assets							
Inventories	63	98	57	164	96	146	146
Trade and other receivables	2,572	3,714	3,206	6,865	8,427	9,427	9,427
Cash	8,321	10,140	11,201	5,646	5,160	6,876	8,318
Total Current Assets	10,956	13,952	14,464	12,675	13,683	16,449	17,891
Current liabilities							
Trade payables	-2,008	-6,461	-4,068	-3,956	-3,902	-5,632	-5,632
Lease liabilities	-112	-86	-94	-78	-164	-164	-164
Deferred income	-2,800	-3,444	-4,677	-3,323	-4,992	-4,500	-4,500
Borrowings	-1,149	-2,073	-1,421	-971	0	0	0
Total Current Liabilities	-6,069	-12,064	-10,260	-8,328	-9,058	-10,296	-10,296
Net Current assets	4,887	1,888	4,204	4,347	4,625	6,153	7,595
Long term liabilities							
Trade & other payables	-139	-402	-143	-100	0	0	0
Lease liabilities	-257	-171	-78	0	-151	0	0
Deferred income	-1,096	-2,705	-2,147	-2,285	-2,491	-2,750	-2,750
Borrowing facility	-1,788	-405	-1,356	-237	0	0	0
Total Long Term Liabilities	-3,280	-3,683	-3,724	-2,622	-2,642	-2,750	-2,750
Net Assets	17,090	13,881	15,803	15,884	16,736	18,372	20,039

Source: Company Accounts, Equity Development estimates

Contacts

Andy Edmond
Direct: 020 7065 2691
Tel: 020 7065 2690
andy@equitydevelopment.co.uk

Hannah Crowe
Direct: 0207 065 2692
Tel: 0207 065 2690
hannah@equitydevelopment.co.uk

Equity Development Limited is regulated by the Financial Conduct Authority

Disclaimer

More information is available on our website www.equitydevelopment.co.uk

Equity Development, 2nd Floor, Park House, 16-18 Finsbury Circus, London EC2M 7EB

Contact: info@equitydevelopment.co.uk020 7065 2690