EDISON

Corero Network Security

Market share gains in an expanding market

Initiation of coverage

Software and comp services

10 November 2025

Corero Network Security is a leading provider of distributed denial-of-service (DDoS) detection and mitigation solutions. Its innovative technology, which is hardware agnostic, offers customers many advantages over other solutions. We expect Corero to achieve market share gains in a growing addressable market. Our valuation analysis suggests upside to the current share price of between 35% and 76%.

Year end	Revenue ($m)	EBITDA ($m)	PBT ($m)	EPS (¢)	EV/sales (x)	EV/EBITDA (x)	P/E (x)
12/23	22.3	2.0	0.1	0.01	2.8	31.5	N/A
12/24	24.6	3.0	1.0	0.16	2.6	21.0	81.6
12/25e	24.7	(0.2)	(2.3)	(0.33)	2.5	N/A	N/A
12/26e	28.7	2.7	0.3	0.05	2.2	23.0	N/A

Note: EBITDA, PBT and EPS are normalised, excluding amortisation of acquired intangibles, exceptional items and share-based payments.

DDoS threats growing in scale, sophistication, intent

DDoS attacks are a relatively easy way for cyber criminals and hacktivists to paralyse the computer networks of their targets and cause major service disruptions. In recent years, helped by an evolving geopolitical landscape, there has been a sharp rise in DDoS attacks, which increased by 50% in 2024. Falling victim to an attack has a huge impact on service providers and their customers, as well as enterprises, most notably reputational damage and material financial consequences.

Corero: Next-generation technology

Corero's innovative technology differs from many others; rather than relying on network traffic pattern recognition, it uses deep packet inspection (DPI) to analyse the data itself. This allows customers to use the solution in a more flexible and cost-effective way. Moreover, Corero's technology is a software solution and is hardware agnostic, allowing customers to implement its products without the cost and inconvenience of making changes to their existing infrastructure.

New management: Positive impact already seen

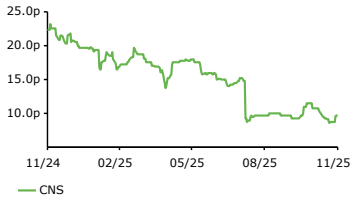
CEO Carl Herberger joined at the start of 2024. An industry veteran with a strong record of revenue expansion, he has restructured the direct sales operations and overseen expanded industry partnerships to enhance indirect selling. New product launches further expand the total addressable market (TAM). The current year has seen a shift in revenue mix as customers increasingly purchase solutions on a subscription model, leading to annual recurring revenue (ARR) growth of +25%. After good order momentum in Q325 management has confirmed FY25 guidance.

Valuation: Market share gain potential not priced in

Although the revenue shift seen in the current year has resulted in reduced near-term expectations, we see this as a positive change in the long term, increasing the visibility of revenues, profits and cash generation. Corero's shares look undervalued. Peer analysis suggests the company is undervalued by c 60%. A discounted cash flow (DCF) implies 76% upside. Applying the 'Rule of 40' and comparing Corero with other high-growth SaaS businesses suggests share price upside of 35%.

Price	**9.65p**
Market cap	**£50m**
Net cash at end June 2025	$3.1m
Shares in issue	512.2m
Free float	32.0%
Code	CNS
Primary exchange	AIM
Secondary exchange	OTCQX

Share price performance



%	1m	3m	12m
Abs	(2.5)	(30.4)	(49.4)
52-week high/low		29.0p	8.8p

Business description

Corero Network Security is a leading provider of DDoS attack detection and mitigation solutions, protecting organisations against external and internal threats and ensuring the ability to continually operate web-based services.

Next events

Q325 trading update	November 2025
FY25 trading update	January 2026

Analysts

Dan Ridsdale +44 (0)20 3077 5700
Neil Steer +44 (0)20 3077 5700

tmt@edisongroup.com
Edison profile page

Investment summary

Corero Network Security is a leading provider of software solutions that help customers combat the growing threat of DDoS attacks. DDoS attacks are designed to direct a high volume of illegitimate data traffic to the computer servers of the target customers, causing their systems to become overloaded and, ultimately, the service to fail. The perpetrators of DDoS attacks have become more sophisticated in recent years, making use of an increasingly complex corporate communications landscape. For example, increasing use of Internet of Things (IoT) devices has allowed perpetrators to infiltrate edge devices with malware to create 'botnets' that generate and direct illegitimate data traffic to targets. Apart from the usual drivers of cybercrime (eg financial gain), the evolving geopolitical landscape in recent years has fuelled a marked increase in DDoS attacks, rising by more than 50% in 2024. Industry forecasts predict that the addressable market for DDoS mitigation solutions ($5.5bn in 2024) will increase at a CAGR of 14% in 2024–30. Corero's products offer certain key benefits over peer group solutions, and we believe it can surpass this industry growth thanks to market share gains.

Financials: Building a platform for better growth and margin expansion

New CEO Carl Herberger joined the business at the start of 2024 and, while Corero performed creditably over the course of the year (delivering 10% revenue growth and 16% ARR growth), the key focus has been on establishing a platform for faster growth. Initiatives include restructuring the direct sales operations and expanding industry partnerships to increase indirect selling, while the introduction of new products further expanded Corero's TAM. Over H125 Corero experienced a marked shift in demand towards subscription (DDoS protection-as-service, DDPaaS) solutions. Market uncertainties as a result of the US tariff changes are believed to have helped drive this change. The result was an increase in ARR of 25% in H125. We see the switch to DDoS PaaS purchases as a long-term positive, increasing revenue visibility and reducing execution risk, even though near-term forecasts are affected. Already in the early stages of H225 there is clear evidence that partnership channels are starting to deliver sizeable opportunities and expansion into new market regions. Beyond the current year, we believe there is a clear opportunity for market share gains, for growth to exceed our estimates and to drive operationally leveraged earnings upside.

Sensitivities

Sensitivities include:

- **Execution risk:** while we believe the current management team has a solid and well-engineered strategy to take the business forward, achieving share gains in an expanding market, our investment thesis relies heavily on the new management team executing well. Early indications are positive, but execution risk exists.
- **Industry partnerships** are a key component of the strategy, with current agreements with Juniper, Akamai and GTT. Of course, sensitivities relating to partnerships work in both directions and, while management needs to maintain existing ones, our forecasts do not include potential upside from any new industry partnerships.
- **Disruptive pricing:** if one or more of Corero's key competitors decided to participate in aggressive price disruption for a prolonged period, it could adversely affect the overall industry segment's TAM.
- **Technology disruption:** Corero's current technology gives it a leading position, something we believe is sustainable. If a new technology emerges, it could affect our forecasts.
- **Consolidation:** Corero's balance sheet is healthy, and it will build a stronger net cash position over time. Management may be tempted to participate in consolidation, which could have a positive or negative impact.

Valuation

We value the business using a variety of techniques. Comparison of multiples (specifically EV/sales) against a peer group of businesses implies share price upside of 60%. Application of the Rule of 40 regression analysis to Corero's valuation when compared to industry peers implies upside of 35%. Given the long-term structural growth, operational leverage and rising cash generation, we believe assessing Corero's value using a DCF model has merit. On our conservative assumptions, our DCF implies 76% upside to the current share price. Finally, we note that the cybersecurity industry has seen, and continues to see, consolidation, with the transactions of listed businesses in recent years commanding a buyer's premium of 35%.

Solutions to mitigate DDoS threats

Please see the Appendix to this note for a description of the DDoS problem, types of DDoS attack and perpetrators as well as industry data on the size and growth of the market.There are several ways to detect and mitigate DDoS attacks, most commonly based on the need to detect specific data traffic patterns and, once suspicion is aroused, directing traffic to be 'scrubbed' before being redirected on its intended route. This traditional method has some inherent challenges. Corero's solution is based on analysis of the data packets themselves and avoids the challenges of scrubbing, offering better accuracy of detection and a more rapid response time.

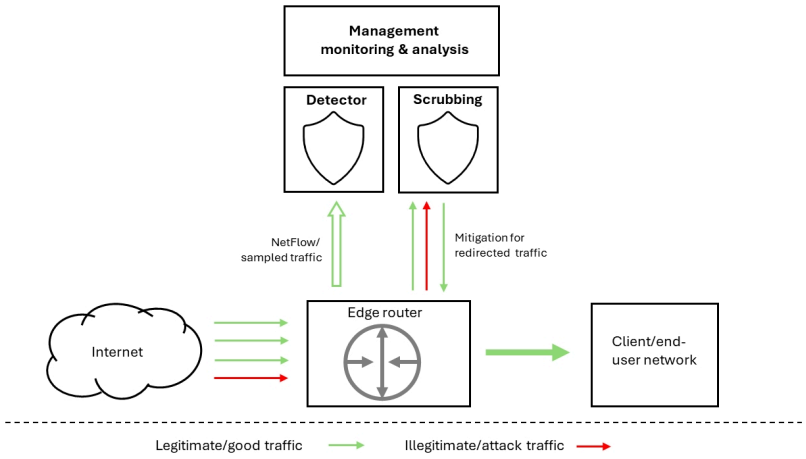
Conventional cloud scrubbing

Cloud scrubbing is a common DDoS mitigation technique. It works by taking all traffic destined to a particular IP address and redirecting it to a particular data centre. At the data centre, the traffic is analysed using various techniques and scrubbed or cleaned so that only verified traffic is forwarded back to the original IP address.

Essentially, the scrubbing process is undertaken according to two basic protocols: either scrubbing all the data continuously or adopting a protocol in which traffic is switched to the scrubbing data centres when believed to be suspicious. The concept of cloud scrubbing has been around for many years and, while a valuable service, providers of cloud scrubbing services to ISPs, hosting companies, cloud application service providers and large corporates tend to provide a one-service-fits-all model.

The structure of a conventional scrubbing service is shown below. As indicated, once 'suspect' traffic is detected, a traditional solution would intervene and direct the traffic to a 'scrubbing' location, which can either be on-premise or cloud-based.

Exhibit 1: Traditional cloud scrubbing



Source: Edison Investment Research

There are some inherent disadvantages of this traditional method, including cost, relatively slow mitigation due to diversion requirements (and manual intervention) and the potential for periods of service latency. Obviously, the latency issue is something to be avoided due to the inevitable impact on the customer user experience.

Moreover, the issue surrounding system latency has become more relevant over the last few years. Typically, once an attack has been detected, most scrubbing protocols will direct all traffic via the scrubbing centre, which affects legitimate as well as illegitimate traffic and users. Given the changing structure and increased complexity of networks (eg the rise in points of access via IoT/5G connectivity), it has become easier for perpetrators to design attacks that are short but repeated. Such attacks are more difficult to detect but, once detected and mitigation via scrubbing services is enabled, they can have a protracted impact on service latency.

A better way: The Corero solution(s)

Corero's methodology for identifying DDoS attack threats is fundamentally different from those based on traffic pattern recognition. Instead, its solutions are based on an analysis of the data packets themselves, through propriety DPI. The

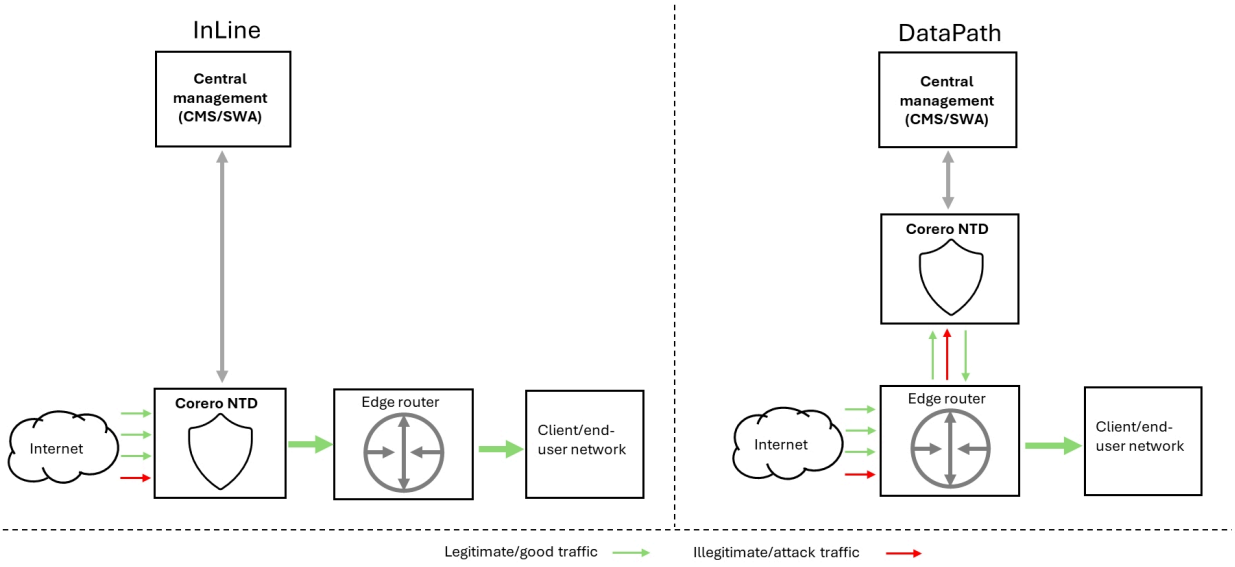
company has developed this technology over the last 15 years as a result of close to $40m in development spend.

DPI is made possible as a result of the way in which the packets of data sent over a network need to adhere to a common set of industry standards. Data packets are made up of three common components: the header, payload and trailer. The header contains a lot of information about the data packet including the type of service, source address, destination address and a time-to-live identifier (which indicates the time a packet is due to remain active in a network before being discarded). The ability to analyse the data header packets, the structure of the data packet payload and the overall protocols used across the data packet is at the core of DPI. This is where Corero's technology excels in developing a DDoS detection and mitigation solution. Corero's product is branded as SmartWall ONE™.

A key advantage of the SmartWall ONE solution is the DPI technology can process network traffic in real time. This allows the solution to be deployed in a way that samples the network traffic received by an entity and detects the source and nature of an intended DDoS attack in real time. Not only is the attack threat typically detected more quickly than other methods, but mitigation, which may vary according to the type of attack, can also be implemented more quickly. Moreover, the ability to continually update and automate the process of detection and mitigation, in contrast to the manual intervention required in scrubbing, means that Corero's technology can be far more cost-effective.

Corero's SmartWall ONE products (Threat Defense System, Threat Defense Director and Edge Threat Defense) can be deployed in several configurations, as indicated below.

Exhibit 2: Corero's approach to DDoS detection and mitigation



Source: Edison Investment Research

The Corero product suite

Corero's products include the SmartWall ONE DDoS protection platform and the SecureWatch suite of managed services. Customers include ISPs, hosting companies as well as cloud and SaaS solution providers. These service providers use Corero's products to safeguard against attacks directly on their own service provision as well as attacks directed at specific customers that they serve.

Corero sells to customers in a flexible format in several ways:

- as an appliance sale and term software licence plus annual SecureWatch services;
- as a software subscription for its virtual appliance software; or
- as a service, which enables the customer to utilise the technology on a subscription or revenue share basis (without owning the appliance and software).

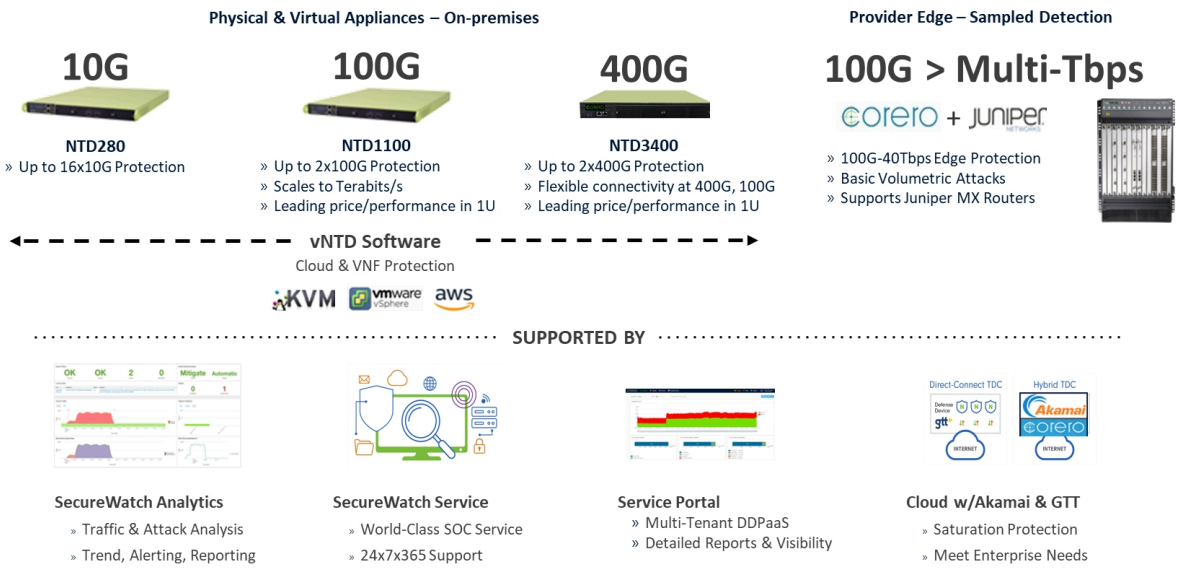
Increasingly, customers engage with Corero to supply the solutions and run and maintain the services over multi-year contracts. Revenues under this model are referred to as DDoS as a service (or DDoS PaaS).

In summary, the key advantages delivered to customers via the SmartWall One product suite and its propriety DPI

technology include:

- **Speed and accuracy of detection:** using the real-time, always-on protection model, the SmartWall ONE suite permanently assesses threats and has the ability to intervene instantaneously. Attacks are mitigated in seconds, and it typically acts faster than other products. Downtime experienced by customers is minimised.
- **Simplicity:** unlike other solutions that are tied to particular hardware platforms, the fact that the core technology of DPI is software-based allows the SmartWall ONE suite to be used in a hardware-agnostic fashion. This leads to a lower total cost of ownership and means that customers face limited installation costs by not having to alter network infrastructure.
- **Flexibility:** SmartWall ONE products can be purchased and deployed in a broad range of models including as an appliance, as edge infrastructure solutions and via cloud-based DDoS services.
- **Scalability:** the very nature of the software-based products means they can be scaled in a modular fashion. Management believes the solutions offer the best price versus performance ratio in the marketplace.
- **Visibility:** it is important to realise that, as well as the products themselves, Corero has a range of services that provide dashboard intelligence and forensic analysis of network traffic before, during and after attacks. These data services can be crucial in providing customers with insights to improve measures against future attacks.
- **Support:** Corero provides support and service contracts with 24-hour, 365 days support. The fact that the company achieves renewal rates of 97–99% for these services is evidence that they are world-class.

Exhibit 3: Corero's SmartWall One product suite



Source: Corero Network Security

The sales strategy and key partnerships

Strategic partnerships with large original equipment manufacturers (OEMs) have been a key part of Corero's sales model for many years. With the arrival of CEO Carl Herberger (in January 2024), an overhaul of the sales strategy was undertaken, including strengthening partnerships as well as augmenting the direct sales team. While the business has already seen some benefit as a result of these changes, we believe it is still early days for the transformation, with the full benefits to come, coinciding with the launch of new products (such as the Corero Observability & Resiliency Ecosystem). For a company with a direct salesforce of 16, Corero's access to a much larger indirect selling channel is one of the business's key strategic merits. We believe that currently around 30% of net revenues are via the partnership channels.

Akamai Technologies: A new agreement with a major industry player

A recent major development was the signing of a global partnership deal with Akamai in September 2023. Akamai started as a Corero customer itself but through this partnership agreement has now agreed to promote and sell Corero's SmartWall ONE on-premise product alongside its Prolexic cloud DDoS product, allowing Akamai to market a hybrid solution using the two products.

With revenues of $4bn, Akamai is a leading provider of cybersecurity and cloud computing solutions. Its adoption of Corero's technology to expand its offering to provide customers with a robust and scalable hybrid solution for DDoS detection and mitigation is a major industry 'seal of approval' for Corero.

Importantly, the partnership is a global agreement and will therefore help Corero to access many new markets. We note that Akamai derives 50% of its revenues from outside the US. For example, it has more than 2,000 customers in the Asia-Pacific region, which is forecast to be the fastest growth region for DDoS detection and mitigation (Markets and Markets Research).

Moreover, Akamai notes (in its investor presentation materials) that 70% of its customers purchase just one of its cybersecurity products, with 20% purchasing three or more. With a clear intention to up-sell and cross-sell new products into its installed customer base, the expansion of offerings specifically based on the back of the partnership with Corero can be seen as a solid alignment of interest for the two businesses.

Juniper Networks: Partnership extension now covers all Corero products

Juniper has been a key partner since 2016 when the two companies entered into a technology alliance. As well as an expansion in Corero's sales reach at the time, after a two-year joint development programme the partnership resulted in the launch of enhanced products in 2018. Since then, the partnership has continued to evolve and in early April 2025 the two companies announced a comprehensive expansion of the partnership that enables Juniper to market and sell Corero's full suite of solutions (including SmartWall ONE and the new cloud native CORE platform) to a much broader range of customers, specifically including customers in a 'multi-vendor' environment. In contrast to the previous agreement, through which Corero's technology was used on one Juniper product, this broader reselling agreement means that the entire range of Corero's solutions can be chosen to replace competitor products.

With revenues of more than $5bn (FY24), Juniper is one of the largest OEMs of network communications equipment, with selling functions globally. In January 2024, Hewlett Packard announced plans to acquire Juniper, but in January 2025 the US Department of Justice announced plans to block the purchase, causing a delay in the merger process, which finally completed in July 2025. Juniper invested in Corero in 2018 and currently has a 9.6% shareholding.

GTT Communications: A tier one ISP

Corero signed a partnership with tier one ISP GTT in 2017. GTT is one of the top five ISPs in terms of traffic volume globally. Since 2017 GTT has used Corero's SmartWall ONE Threat Defense System as its platform for DDoS mitigation, a service sold to its customers, along with IP transit services. Since the initial partnership deal, the relationship has strengthened and in 2023 GTT announced an expansion of its global scrubbing centre capacity and network in which Corero's SmartWall ONE technology will be used for DDoS detection.

TechEnabler: Opening up distribution channels to the Latin America region

In February 2024, Corero announced a new strategic partnership with TechEnabler, a leading service provider in Brazil, with the intention of expanding Corero's footprint in the Latin American (LatAm) region, a region in which the business had limited exposure until that point. The announcement of the strategic partnership was simultaneous with confirmation that Corero had booked more than $1m in order intake for products and services, including SmartWall ONE, as part of TechEnabler's scrubbing-as-a-service offering for end user Forte Telecom.

In April 2025, TechEnabler and Corero announced a further strengthening of their partnership to include use of the latest SmartWall ONE (400G) platform across TechEnabler's network to offer DDoS protection-as-a-service. As well as end user Forte Telecom, the partnership has resulted in Corero's products and services being used by other local operators including DigitalnetBR.

New management, supported by a highly experienced board

Corero's management has substantially changed over the last 18 months, with the appointment of a new CEO and CFO. However, the new management team is supported by a very stable board, which includes several long-serving veterans of the technology industry. The very entrepreneurial (non-executive) chairman (Jens Montanana) is a major shareholder. Having joined the business at the start of 2024, over a short period of time the new CEO Carl Herberger has made a marked impact in terms of sales strategy and new product introduction. Supported by the experienced board, we believe the senior management team has the experience, skill and shared interests to develop the business and drive shareholder value.

Carl Herberger (CEO) was announced as the new CEO in November 2023 and joined the board on 1 January 2024. Carl brings over 25 years of cybersecurity leadership experience as an internationally recognised expert in the field. He has held executive roles at top security firms including Radware. Among Carl's many achievements, he received the Technology Executive of the Year award in 2019 and helped establish the US Air Force's first cyber warfare unit during his time as an intelligence officer. As CEO, he leverages his deep expertise across all facets of cybersecurity to lead Corero's corporate strategy and help its customers manage risk and build resilient systems capable of withstanding today's cyber threats.

Chris Goulden (CFO) joined in May 2024 after 12 years at CBRE Group, where he held a number of senior positions including finance director for the UK and more recently finance director for the Central Europe and Nordics regions. Prior to this, Chris held a number of roles over a period of three years at BNP Paribas. He qualified as an accountant with Ernst & Young.

Jens Montanana (non-executive chairman) is the CEO of Datatec, which he founded in 1986, and under his stewardship it has grown to be an established international ICT solutions and services company operating in more than 50 countries. Datatec listed on the Johannesburg Stock Exchange in 1994. Jens has spent the majority of his more than 30-year career in the technology industry, with considerable operational and commercial experience in the resale and distribution of information technology hardware and software solutions.

Andrew Miller (non-independent, non-executive director) served as Corero's CFO from 2010 to 2019. Until February 2025, he was CFO of Mycom, a telecoms SaaS provider, and previously CFO and COO of C5 Capital, an investment firm investing in the secure data ecosystem including cybersecurity, cloud infrastructure, data analytics and space, and CFO of Haven Group, a private equity-backed cybersecurity services provider.

Richard Last (independent non-executive director) has over 20 years' experience in information technology, having worked at board level for a number of publicly quoted and private companies in the technology sector. He is a Fellow of the Institute of Chartered Accountants in England and Wales. Richard is currently executive chair at Iomart, a leading provider of cloud managed services.

Peter George (independent non-executive director) has a successful track record as CEO of leading IT network and security companies and provides sales and marketing leadership experience to the board. Until late 2024, Peter was the CEO of Evolv Technology, a US-based leader in human security screening. Prior to that he was president and CEO of empow cybersecurity, a market innovator in AI, machine learning and advanced security analytics.

Rob Scott (independent non-executive director) currently serves as managing director of strategic relationships for venture lending at Avid Bank, leveraging his extensive industry expertise and strong connections with venture capital and private equity firms. He is a member of the customer advisory board at Fortinet, a global leader in cybersecurity. Previously, Rob served as CEO of Cygilant, a cybersecurity services provider that specialised in helping organisations hunt, detect and respond to cyberthreats. After its acquisition by SilverSky, he transitioned to the role of chief strategy officer with a focus on strategic partnerships. Rob currently serves as the chair of Trilio, a provider of data protection and recovery solutions.

The addressable market opportunity

The market for DDoS detection and mitigation services is estimated to be worth just over US$6bn in the current year and is forecast to grow at a rate of around 13% (Markets and Markets Research, see Exhibit 4 below).

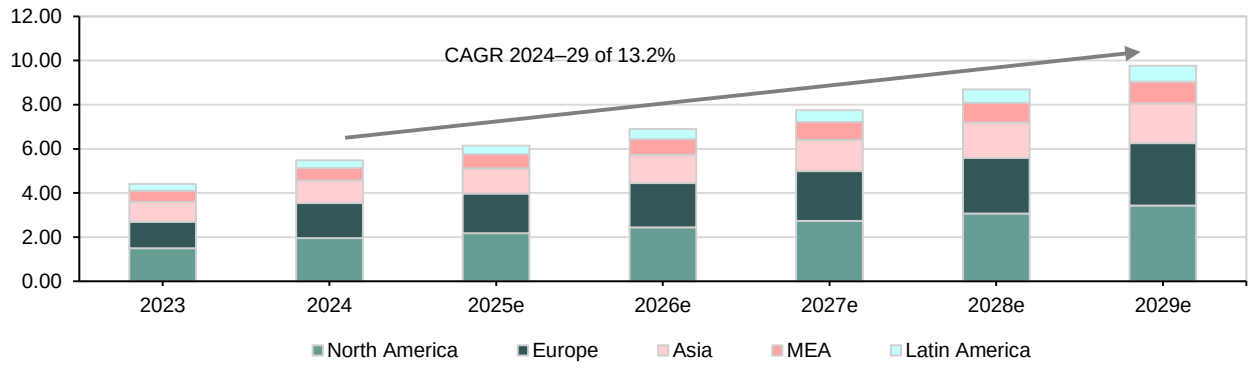
Overall, the US remains the largest region for DDoS detection and mitigation services, representing around one-third of the market. This is believed to be primarily due to the region's general leadership in advanced technologies and strict implementation of cybersecurity generally across all industries in accordance with stringent regulatory and compliance requirements. For example, cloud adoption of enterprise application services in the US is typically ahead of other parts of the world leading to a high concentration of data centres. The ecosystem around mission-critical SaaS service provision has been forced to leverage state-of-the-art cybersecurity products including DDoS mitigation services.

The European region is the second-largest market, accounting for 29% as of 2024. In recent years, the region has shown above trend growth, with a rising focus on cybersecurity, as the regulatory regime has evolved (eg General Data Protection Regulation) and of course as SaaS adoption of mission-critical services plays 'catch up' with the US.

The Asia-Pacific region, currently just under 20% of the market, is expected to see above-trend expansion over the medium term, growing closer to 20%. This is due to the rapid pace of major digital transformation initiatives across the region generally and at the same time the region is seeing a marked increase in the growth of DDoS attacks. Attacks are believed to have been made easier to orchestrate thanks to the proliferation of IoT devices, a high proportion of which are unsecured, thereby facilitating the creation of botnets. We note Corero's plans to strategically increase its sales presence in the region.

In the remaining regions of LatAm and the Middle East & Africa (MEA), growth is also expected to be a little above trend, a direct consequence of increasing internet service penetration, rising digital services adoption and continued catch-up in the use of mobile devices compared to more developed markets. Some regions can be expected to see dramatic expansion, with some forecasts pointing to the Middle East (United Arab Emirates and Saudi Arabia) in particular as likely to show dramatic growth given the pace at which the 'new' digital economies are expanding, encouraged by the longer-term objective of reducing reliance on the oil and gas industries.

Exhibit 4: DDoS mitigation and detection market, $bn



Source: Aggregated Industry Data, Edison Investment Research

Exhibit 29 shows a breakdown of DDoS detection and mitigation spend by industry sector and a clear profile of the threat landscape, with IT & telecom service providers (ISPs etc) accounting for the largest spend. Unsurprisingly, given that this is a market in which geopolitical tensions are known to be a key driver, spend (and attacks) is clearly focused on industry segments most at risk of causing societal harm. We expect this pattern to remain largely unchanged.

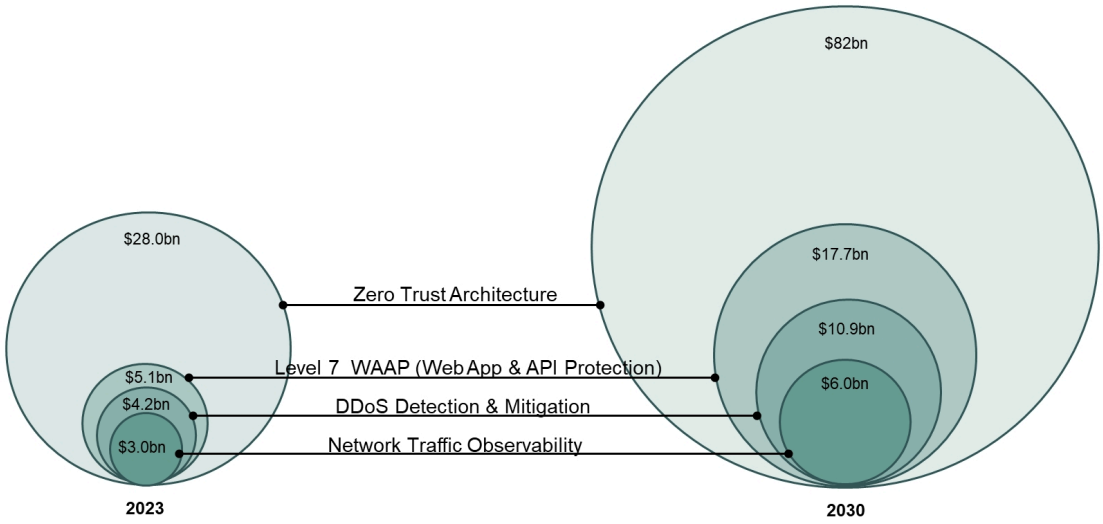
New products: CORE and 400G SmartWall ONE

Corero CORE: launched in October 2024, the Corero Observability & Resiliency Ecosystem (CORE) is a new product that accesses Corero's in-house business data, together with feeds from third-party data lakes, to create a new pre-emptive attack defence platform. For enterprises and service providers, the CORE platform has market leading capabilities including Traffic Analysis, Zero Trust Admission Control and Layer 7 DDoS protection, solutions in demand from Corero's target market, which complement the existing suite of Corero products.

Driven by the access to large data lakes, CORE uses artificial intelligence (AI) and machine learning (ML) to offer insights into potential threats in a pre-emptive manner, allowing customers to better coordinate defence measures across their organisation. Consistent with Corero's technical philosophy, CORE is hardware-agnostic and can be readily integrated with third-party solutions, allowing customers to avoid the time delays and cost of modifying installed infrastructure.

CORE is significant in Corero's addressable market opportunity, driven by the benefits of offering a holistic approach to network data governance. The concept of a Zero Trust network architecture (in which strict identity and verification protocols are in place for every person and device trying to access network resources, regardless of whether that person or device resides inside or outside the network perimeter) requires such a holistic view of network traffic. CORE provides this, as well as the intelligence to become a key component of Zero Trust Network Architecture. Despite only being launched in late 2024, management noted on the Q125 results call (3 April) an expectation that CORE could account for 5–10% of order intake. In reality this proved conservative, with two large orders (totalling $1.8m and representing 14% of H125 order intake) were booked in June.

Exhibit 5: The CORE product and expansion of Corero's TAM



Source: Corero Network Security, Edison Investment Research

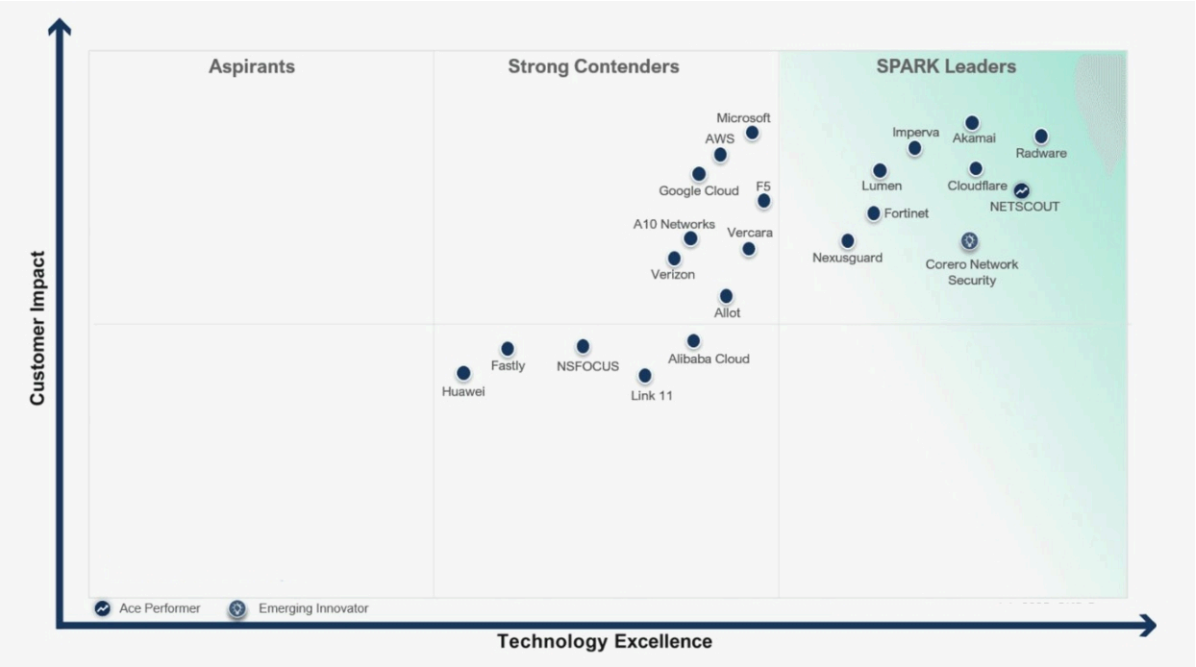
Another recent product enhancement is the introduction of an **extended Web Application Firewall (WAF) and application security for service providers**. We believe this could be a significant new product enhancement and could play an important part in Corero's expansion into large service providers. Traditionally, many peer group WAF solutions have been engineered for use by enterprises directly. In recent years, corporate IT infrastructure has evolved rapidly with a greater reliance on data centres for both data storage and application tenancy. The Corero WAF is engineered to be used by data centre operators in a true multi-tenanted manner. As such, the product allows operators to use the Corero WAF to create new, chargeable services to their own customers.

Corero NTD 3400: in October 2024, Corero launched SmartWall ONE Network Threat Defense (NTD) 3400. This is a new 400G version of the hardware appliance that offers four times the connectivity of previous models but uses less than twice the power consumption. Aside from the performance benefits, the NTD 3400 helps streamline network infrastructure with reduced hardware complexity, flexible deployment options and future-proof scalability.

The innovation was also applied to the sales and marketing of the new product, with the company introducing a new trade-in programme through which customers can upgrade to the new product from their existing 'legacy' Corero solutions. Importantly, the trade-in programme also applies to competitor products, helping Corero drive further revenue opportunities through market share gains.

Given the above product innovations, it is not a surprise that Corero has recently been recognised as a leading innovator in the DDoS detection and mitigation market (Exhibit 10 below). The assessment, undertaken by QKS Group, noted Corero's solutions' remarkable scalability, low-latency protection times, comprehensive range of built-in analytics, as well as its ability to detect attacks from a full range of vectors. Interestingly, the only material challenge noted by QKS Group was a requirement for Corero to offer a WAF, something that has now been addressed as noted above.

Exhibit 6: Corero's market position: Spark matrix for DDoS mitigation, Q325



Source: QKS Group, Corero Network Security

The competitive landscape

There are many suppliers of DDoS detection and mitigation services. However, most providers' solutions rely on assessing network data traffic patterns and looking at anomalies and suspicious patterns to instigate a mitigation strategy. These solutions can be useful for large-scale cloud scrubbing services. However, at the enterprise level, a better hybrid model is desirable to try and accommodate specific end-user requirements. Below we briefly describe the businesses that Corero management views as its key competitors in this market segment, some of which also use DPI as a core technology:

- **Radware:** headquartered in Israel and with a market capitalisation of more than $900m, Radware was formed in 1997 and is listed on Nasdaq. 2024 revenue was $275m, showing 5% growth over the prior year. Its non-GAAP EBITDA margin in 2024 was 12.6%, up from 6.7% in the prior year. The business showed generally consistent revenue expansion in 2011–21 but in the last couple of years has seen more volatile revenues, for example a decline of 11% in 2023 from a peak of $293.4m in 2022. Radware operates 21 scrubbing centres around the world and has DDoS mitigation and protection as a key product, but offers a range of other services including application delivery and performance solutions, as well as application and API protection. The company's global infrastructure of 21 scrubbing centres (over 15Tbps capacity) does provide the business with some strategic advantages over other traditional peers as it offers flexibility and capabilities to divert traffic where required. However, we note that compared with the technical advantages inherent in the Corero product (based on DPI), Radware's services generally still have a higher cost of ownership for customers that are ultimately paying to support this global scrubbing centre infrastructure.
- **Arbor Networks:** founded in 2000, the business resulted from a University of Michigan research project sponsored by DARPA, Cisco and Intel. Arbor Networks was acquired by Danaher Corporation in 2010 but then sold to current owner NetScout Systems in 2015. NetScout is listed on Nasdaq, with a market cap of $1.5bn and group revenue of $830m in 2024. Since the change in ownership in 2010, it has been harder to trace the precise revenue profile of the business, but we believe current revenues are in the range of $180–200m. Like Radware, Arbor operates a global network of scrubbing centres (16 in total) offering over 15Tbps in capacity. It has strategic partnerships with Juniper Networks, Cisco and IBM. Arbor also has its own DPI technology, which it uses in its solutions, and is therefore technically Corero's closest industry peer.
- **F5:** based in Seattle, Washington, and listed on Nasdaq, F5 has annual revenue of $2.8bn and a market cap of $15bn. It provides a wide range of application delivery solutions (eg load balancing, network optimisation and

content caching), as well as application security solutions (web application firewalls, access control solutions and DDoS protection). F5 has been a very active consolidator in the market, averaging one sizeable purchase a year since 2019. In 2014, the purchase of Defense.Net added cloud-based DDoS services to its existing on-premise solutions. Overall, we estimate that DDoS defence and mitigation services represent $140–160m, or 5% of group revenues.

- **A10 Networks:** founded in 2007 and established to serve the identity/access management segment of the IT security market, A10 Networks has expanded its range of solutions via organic development and purchase. It listed on Nasdaq in 2014 and has a market cap of $1.2bn. It achieved revenue in CY24 of $262m (up 4%), with a non-GAAP EBITDA margin of 28%. We estimate that revenue from DDoS detection and mitigation is similar to that of F5 (c $140–160m).

Sensitivities

Corero's sensitivities include the following:

- **Execution risk:** while we believe that the management team has a solid and well-engineered strategy to take the business forward, achieving market share gains in an expanding industry segment, our investment thesis relies heavily on the management team executing well. We take comfort from early positive indications, but execution risk exists.
- **Industry partnerships:** related to the above, a specific component of the strategy concerns the industry partnership agreements with leading players such as Juniper, Akamai and GTT. Sensitivities apply in both directions and, while management needs to maintain existing partnerships, our forecasts do not include potential material upside if additional industry partnerships are forged.
- **Disruptive pricing:** so far, pricing trends around DDoS detection and mitigation solutions have followed the technology industry norm, in which prices per unit data show annual deflation, but this is more than compensated by growth in data volumes and the increased value-add of the solutions. This established trend in many technology market segments allows an opportunity for the providers to up-sell, a key component of the overall expansion in the TAM. If one or more of Corero's key competitors decides to participate in aggressive price disruption for a prolonged period of time, it could adversely affect the overall industry segment TAM, as well as Corero's financial performance.
- **Technology disruption:** we believe Corero's leading technology is a sustainable advantage and will help market share gains. As with all leading-edge technology solutions, there are risks that peers will catch up with or overtake Corero with new technology.
- **Consolidation:** the industry for cybersecurity solutions has shown much consolidation already, but this consolidation continues. Corero's balance sheet is healthy and it will build a stronger net cash position over time. While we believe the business can achieve its longer-term objectives on a standalone basis, management may be tempted to participate in consolidation, which could have a positive or a negative impact on our forecast and valuation assumptions.

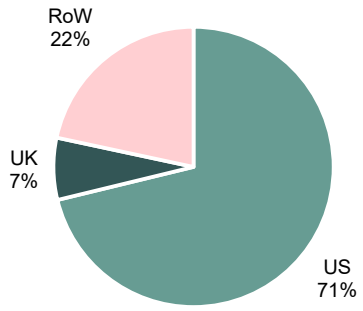
Financials

Revenue profile

Corero's revenues reflect the more developed market for cyber solutions and defence in the US, which accounts for just over 70% of revenues. However, as previously noted, while the US is expected to sustain attractive long-term growth, we expect sales initiatives in certain regions like Asia-Pacific to see a very gradual decline in the face of a dominant US revenue contribution.

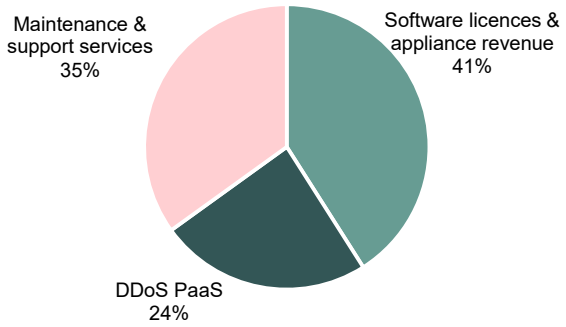
Solutions are sold either through an upfront licence (and maintenance) or through a DDoS SaaS/PaaS model. As indicated, around 60% of revenues are recurrent in nature and, with existing customer renewal rates (by customer number) at 97–98% for both DDoS PaaS and maintenance, forward visibility on revenues is high.

Exhibit 7: Corero revenue by region (FY24)



Source: Corero Network Security

Exhibit 8: Corero revenue by type (FY24)

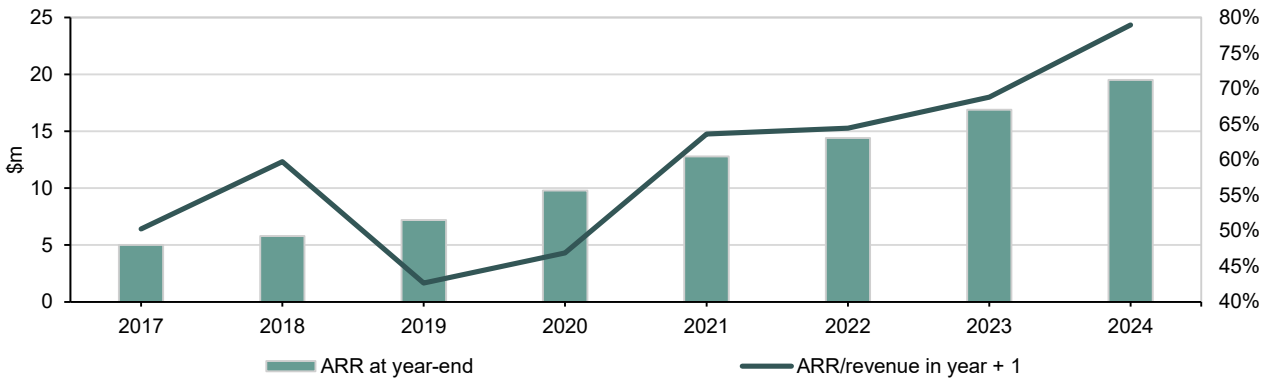


Source: Corero Network Security

Growth in recurring revenue supports visibility

Corero does not disclose renewal by value from existing customers, but we are confident that after inevitable up-selling and cross-selling opportunities, renewals by value each year are comfortably in excess of 100%. As such, ARR at the end of each year represents an increasing proportion of that year's revenue. More importantly, as we show below, ARR also increases as a proportion of the following year's revenue, demonstrating increased revenue visibility over time.

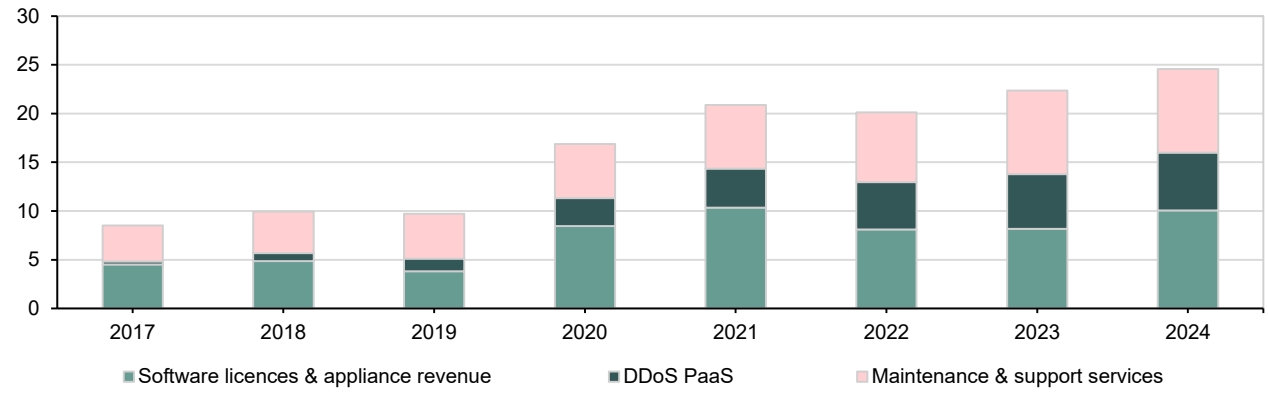
Exhibit 9: Increasing revenue visibility, ARR ($m) at year end and as a percentage of next year revenues



Source: Corero Network Security, Edison Investment Research

This rise in ARR and consequent increase in forward visibility of the business is largely driven by the success of the DDoS PaaS offering, which grew in 2017–24 at a CAGR of 43% and in 2024 represented 24% of group revenue.

Exhibit 10: Revenues by type ($m, 2017–24) – the rise of DDoS PaaS

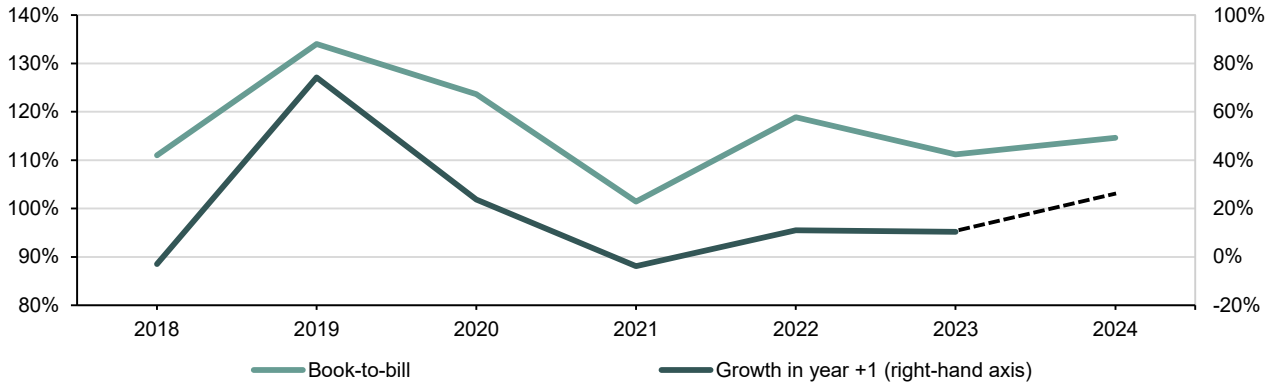


Source: Corero Network Security, Edison Investment Research

Another consequence of the business model and revenue profile is the correlation seen between the annual book-

to-bill ratio (total order intake or 'bookings' divided by the revenues 'billed' in the year) and the revenue growth in the subsequent 12-month period (Exhibit 11 below). We note that in 2024, record order intake of $28.2m equated to a healthy year-on-year rise in the book-to-bill ratio. Based on the historical precedent, we see this as an encouraging lead indicator for an uptick in revenue growth in the current year.

Exhibit 11: Book-to-bill ratio in year and revenue growth in year +1



Source: Corero Network Security, Edison Investment Research

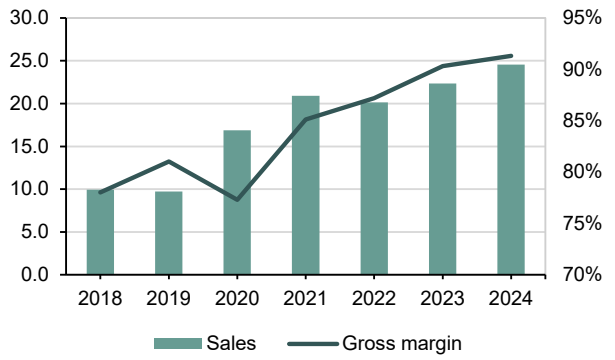
Operational gearing yet to be fully seen

As indicated, impressive operational leverage has been seen in recent years, with sales expansion accompanied by rising gross margin. In 2021–24, the operational gearing inherent in the business model was not seen in the adjusted EBITDA and adjusted EBIT margins, but it is important to recognise a number of factors that prevented this and that are less likely to hold back margin improvements in the future.

- **Sales and marketing:** we estimate that sales and marketing expenses represent close to 50% of overall group opex (FY24: $20m). There has been a marked increase in this expense over the last few years, including an increase in 2024 of more than 40%. Moreover, changes in the sales teams and the addition of new sales headcount in certain regions (LatAm, Asia-Pacific, Middle East and Europe) have added cost over and above revenue growth. The selling efficiency of these new additions, particularly those added over the last year, is invariably not yet at an optimum level, which we expect to be achieved over the coming year. We note that expansion of the sales team has continued into the current year (the direct headcount is now 16 vs 14 at end FY24), but the level of cost addition and change is proportionally less than in the past and not expected to hold back operational leverage in the same way.
- **Restructuring/exceptional expenses:** unlike many technology companies that take charges 'below the line' for restructuring items, Corero's conservative accounting simply absorbs these expenses. On arrival, the new CEO made a number of operational changes to the business that will have given rise to one-off costs (eg charges relating to headcount changes among senior sales executives) and these are all included in operating expenses.

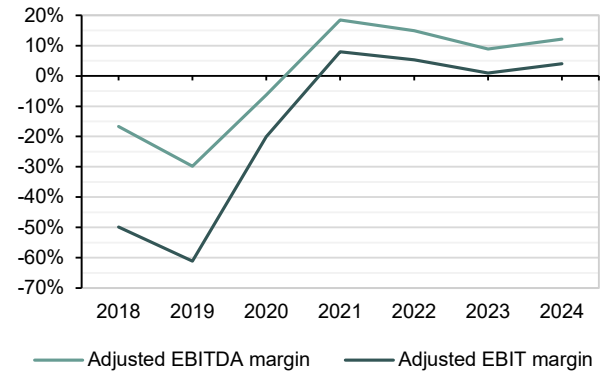
Our forecasts are shown in Exhibit 25. While we expect the business to continue to invest to support revenue expansion ahead of market growth, we expect the adjusted EBITDA and adjusted EBIT margins to show steady increases. We expect an FY27 adjusted EBITDA margin of 15% (vs 12% in FY24).

Exhibit 12: Sales ($m) and gross margins



Source: Corero Network Security

Exhibit 13: Adjusted EBITDA and adjusted EBIT margins



Source: Corero Network Security

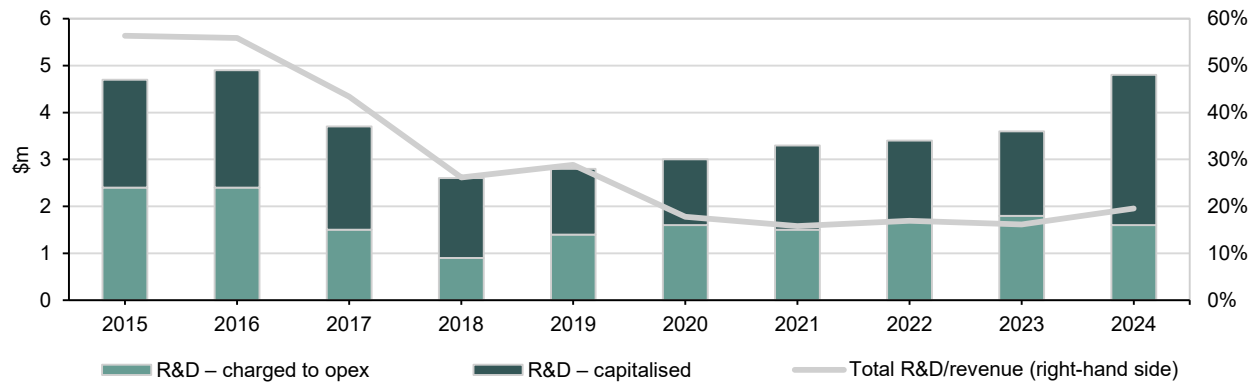
Research and development spend

Sustained high levels of investment in product R&D have been critical to the success and technical advantages of Corero's products. While the company capitalises some product R&D spend, each year there is a significant spend that is taken as cost through the P&L. Exhibit 18 shows the total 'cash' expenditure on R&D as a percentage of revenue each year.

During the development of the SmartWall ONE product (2012 onwards) and for several years post the product launch (H114), there was elevated R&D spend as a percentage of revenue, reflecting the commitment to establishing innovative and market-leading technology. In more recent periods, the ratio of development spend to revenue has settled at a still impressive level of just under 20%.

In 2024, capitalised development spend increased to $3.2m (from $1.8m) due to additional spend on upgrading the SmartWall ONE product for 400G capacity, investments in the new CORE platform and additional spend on the threat research team.

Exhibit 14: R&D spend, 2015–24 ($m)

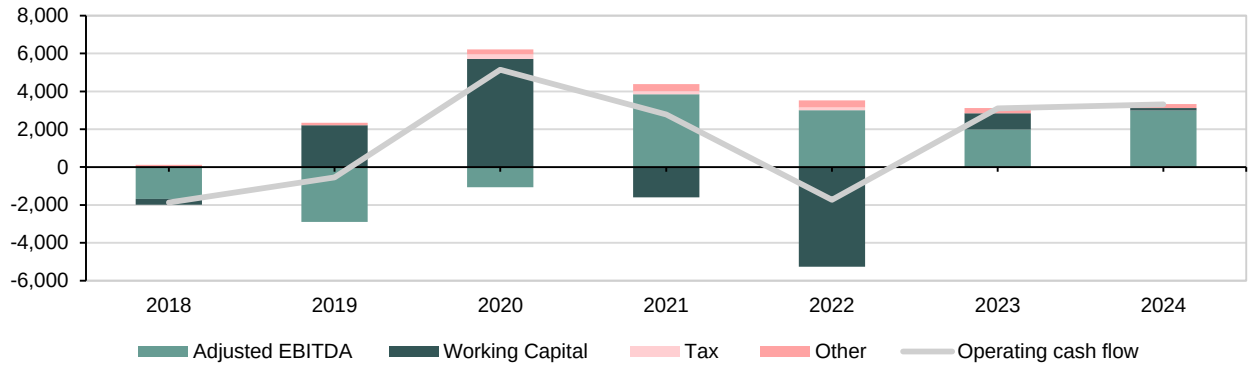


Source: Corero Network Security, Edison Investment Research

Cash generation

As Corero's EBITDA has moved into positive territory in recent years, there has been a marked increase in operating cash flow, which would have been positive in each of the last five years had it not been for a relatively large movement in trade receivables in 2022. This was essentially the final unwinding of favourable payment terms achieved through the earlier stages of the pandemic. There has been a more normalised movement in working capital in the last two years.

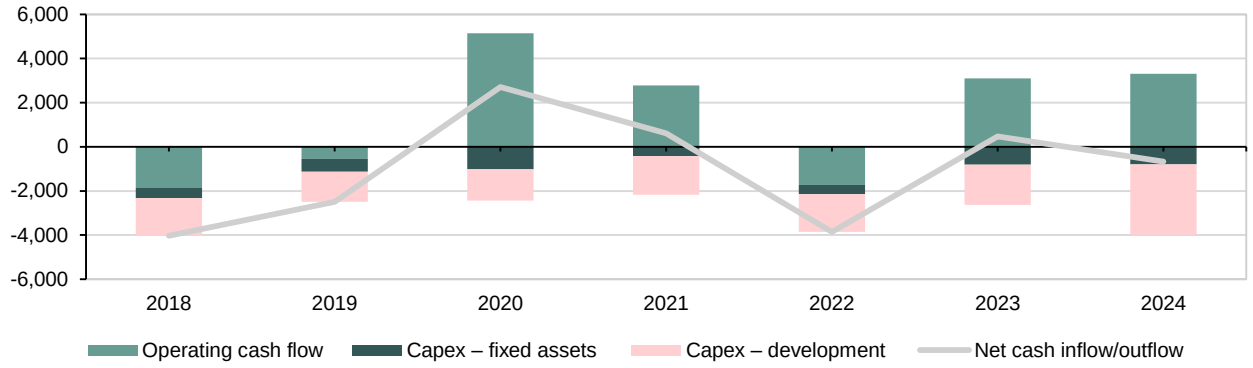
Exhibit 15: Cash flow from operations, 2018–24 ($000s)



Source: Corero Network Solutions, Edison Investment Research

This improving trend in operating cash flow has allowed Corero to sustain the required investments noted above in both software development and fixed asset capital expenditure, with overall free cash flow close to break-even in recent years. A shift towards subscription payments will see a modest net cash outflow in the current year, leaving year-end net cash at $2.3m. However, beyond the current year we expect a steady improvement in free cash flow generation as discussed below.

Exhibit 16: Corero – components of free cash flow, 2018–24 ($000s)



Source: Corero Network Security, Edison Investment Research

Performance in H125

On 16 July, management released a trading update that highlighted a marked change in the order and revenue mix over the course of H125, with more customers choosing to purchase on a subscription model. While this change is positive for the business in the longer term, as it increases the predictability of revenues, profitability and cash generation, there was nevertheless an adverse impact on near-term forecasts.

A shift to subscriptions

Historically, Corero has offered customers the option to purchase solutions in two different ways. The first of these is a traditional capex model in which customers pay an initial fee for software and any required hardware, followed by an annual maintenance fee. In recent years, this model has accounted for around c 40% of group revenues, with a further 25% generated from DDoS PaaS subscriptions and the remainder (35%) from maintenance contracts and the provision of other support services.

In the early part of 2025, market uncertainties emerged as a result of the US trade tariff changes. The disruption and uncertainty was seen broadly across many markets, often creating a change in the way in which customers purchased goods and services. According to E&Y, there was a 20% increase in the number of profit warnings issued by UK registered businesses over Q1–Q225, with 46% off all warnings specifically citing geopolitical tension and policy changes as the key factor.

Although Corero's products were not directly affected by tariff changes, overall customer spending preferences are believed to have adapted, as seen by a greater appetite for subscriptions. Management also believe that, as a number of its competitors had moved to only selling on a subscription basis, customer benchmarking of solutions will have inevitably encouraged a comparison with (and subsequent purchase of) Corero's own DDoS PaaS subscription service. This contributed to a 25% increase in ARR over H125 and saw traditional software and appliance revenues fall from 40% to 29% of group revenues.

Channel partner performance

The benefits of the expanded channel partner agreements are expected to be material in due course, but several one-off factors over H125 resulted in performance being below management's expectations.

The merger of HP and Juniper, which was originally announced in January 2024, was only concluded in July of this year, having been delayed as a result of the Department of Justice lawsuit filed in January. The delays in the integration process of the two businesses is believed to have affected partnership-driven sales over H125. This issue is now fully resolved.

The partnership with Akamai involves Corero's on-premise solution being sold as a complementary product alongside Akamai's cloud-based product, creating an 'always-on' solution, increasingly required in certain enterprise applications. With a slightly more complex selling process, some early inertia was seen, meaning the full revenue benefits from this partnership were not seen over H125. However, in its 28 August press release, Corero announced a multi-year deal with a large European financial institution secured with Akamai. This is discussed in more detail below and is expected to be a template for more substantial enterprise deals in due course.

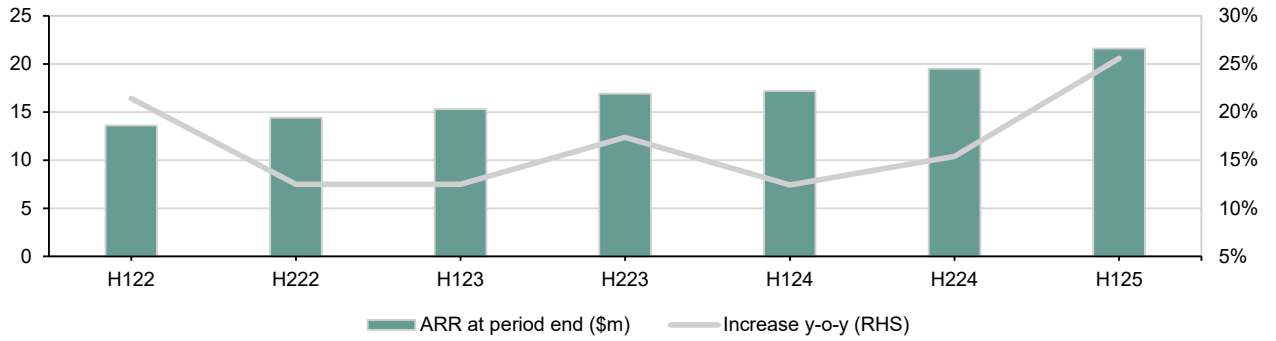
H125 results: Key metrics

Order intake and ARR

Order intake at $12.5m was down 12% y-o-y. Orders were notably soft in Q125 (down 35% y-o-y) with the aforementioned factors being heavily influenced by customer delays and uncertainties in light of trade tariff changes. Encouragingly, a marked improvement was seen in Q225, with order intake up 13% y-o-y, helped by some encouraging new business wins for the recently introduced CORE product.

The shift towards the DDoS PaaS was seen with a substantial increase in ARR levels, which were up 25% to $21.5m at the end of H125. As indicated below, this is the most pronounced increase seen in ARR in recent years.

Exhibit 17: Corero ARR increases year-on-year, H122–H125



Source: Corero Network Security, Edison Investment Research

Revenues

For H125 revenues were down 10% to $10.9m (from $12.2m in H124) due to the factors noted above. Management noted that the shift towards DDoS PaaS purchasing accounted for $1.3m of the revenue shortfall.

Revenues by activity clearly reflected the demand shift, with software licence and appliance revenues down 38% y-o-y in H125, while the DDoS PaaS revenues increased 10%. DDoS PaaS revenues represented 30% of revenues in the period, an increase from 24% in FY24. Maintenance and support revenues showed a healthy increase of 9% y-o-y in H125.

Margins and profitability

Despite the shift in demand and the change in revenue mix, gross margins remained robust at an impressive level of 91%. Having invested heavily in the expansion of the sales team over the last year, overall operating expenses increased 9% to $11.3m. As a result, adjusted operating profit (before stock-based compensation) was a loss of $2.2m in H125 compared to the business running at break-even in H124.

With depreciation and amortisation of intangible assets unchanged at $1.0m, the adjusted EBITDA in H125 was a loss of $1.3m compared to a profit of $1.0m in H124.

Cash flow and balance sheet

The shift in customer purchasing has had a small impact on the cash generation, with the traditionally strong cash collections over the first half of the year adversely affected. As a result, in H125, cash generated from working capital was reduced and, with the operating loss, this led to an operating cash outflow of $0.6m compared to operating cash inflows of $3.7m in H124.

Investments in new products continue and we note the 33% increase in capitalised software development spend to $1.4m. Together with other fixed assets investments and the operating cash outflows, this led to an overall net cash outflow of $1.9m. Net cash, therefore, at the end of H125 was $3.1m, down from $5.3m at the end of last year.

Management has commented that the business is in the advanced stages of finalising an overdraft facility, which is clearly a prudent move given the impact seen on cash generation from the shift to DDoS PaaS procurement. However, our forecasts suggest the business will remain in a net cash position over the next three years.

New business wins

While challenges were seen in H125, there were, nevertheless, some sizeable new deals signed, including:

- a $1.5m contract that sees the expansion of Corero's relationship with TierPoint, including the deployment of Corero's new CORE product;
- a three-year contract of $1.2m with Forte Telecom, one of the largest telecommunications providers in Rio de Janeiro, Brazil;
- a five-year expansion contract valued at $1.2m with existing customer LightEdge, which will see Corero's protection solutions used across LightEdge data centres as a replacement for an incumbent DDoS provider;
- a $0.8m contract renewal and extension with TechEnabler, a leading managed service provider for enterprise and telecommunications networks in Brazil; and
- a $0.3m contract with Cooper Health, which will incorporate Corero's new CORE zero trust admission control capabilities across almost 14,000 employees working across three hospitals.

Momentum continues through H225 with a key customer renewal and expansion in Q4

In addition to the above deals, which all closed in H125, the order momentum has continued over the course of Q325 and into Q425.

On 28 August, Corero announced a multi-year deal with a large European financial institution, secured with partner Akamai. We believe this deal is material but, perhaps more importantly, it demonstrates how, via the partnership, Corero has been selected for a large enterprise customer, representing a shift away from the historical focus on service providers. We understand that the financial institution has concluded that today's threat environment requires a more comprehensive or 'holistic' approach to DDoS protection and mitigation, choosing to combine Akamai's cloud product with Corero's on-premise threat detection solution. This is another example of Corero displacing a peer product, demonstrating the opportunities that exist through the pursuit of one of Corero's key strategic ambitions of targeting competitor displacements.

This new business is believed to be a direct consequence of new EU legislation that covers all financial services companies globally that have any operations in EU markets. The Digital Operational Resiliency Act (DORA) came into effect in January 2025 and sets a much tighter regulatory and reporting framework for all financial institutions (banks, credit institutions, crypto-asset-backed providers and crowdfunding platforms) to ensure critical services are more robust and are able to cope with the increased threat of cyberattacks. The scope of DORA extends beyond the financial institutions themselves and also covers their ICT third-party providers. Having seen one major bank upgrade its cyber

defences and deploy Corero's DDoS solutions, management is optimistic similar new business wins can be achieved.

Including the above deal, a Q325 trading update (released on 5 November 2025) confirmed that new contract wins secured across the US, the UK, Europe, Brazil and Singapore led to an overall order intake in Q325 of $7.4m. This was an increase of 23% on Q224 and included two further new CORE customer wins.

The trading update also confirmed the strong momentum has continued into Q4 with a key customer, a US cloud computing provider, renewing and expanding its contract. The contract, to use Corero's solutions to provide DDoS protection to current and planned data centre capacity, has a contract value of $6.8m, of which only $0.8m was included in the Q325 order intake figure. The contract includes $3.1m of renewals (all existing contracts) and an expansion of $3.7m.

Forecasts

Revenue growth

In the current year, after the challenges experienced in the first half, we expect a marked recovery in H225, with revenue growth of 11%. This will result in full-year revenues being little changed (+1%) from those achieved in 2024. With a much more beneficial tailwind from the new strategic partnerships, beyond the current year, we expect further market share gains to be achieved, most notably in several of the newer regions. This should lead to growth ahead of the industry. We forecast revenue expansion of 16% in 2026, followed by 17% in 2027. We believe these are conservative assumptions and that continued success in both the enhanced sales strategies and new product introductions (eg CORE) leave scope for revenue forecast upgrades in due course.

Margins

In the last couple of years, Corero has invested in new products, re-engineered sales operations and incurred some one-off expenditures. As a result, while revenues have expanded with an improving gross margin, the 'drop-through' to the adjusted EBITDA margin has been somewhat hindered. The current year has now seen the adverse effects on revenues from higher DDoS PaaS adoption, while investments made in the sales team expansion last year have also had to be borne by the business. The result is that we expect a small adjusted EBITDA loss in the current year. As indicated in Exhibit 22, we expect to see the inherent operational leverage and adjusted EBITDA margin expansion in subsequent periods. Our forecasts allow for management to continue investing in both new products and expansion of the sales team capabilities to achieve market share gains.

Company guidance for 2025

Our profit and loss forecasts for the current year sit comfortably within management's guidance of FY25 revenues of $24.0–25.5m and an EBITDA loss between $1.5m and $0m. This FY25 guidance was reaffirmed in the Q325 trading update released on 5 November.

Exhibit 18: Key forecast metrics, 2024–27e

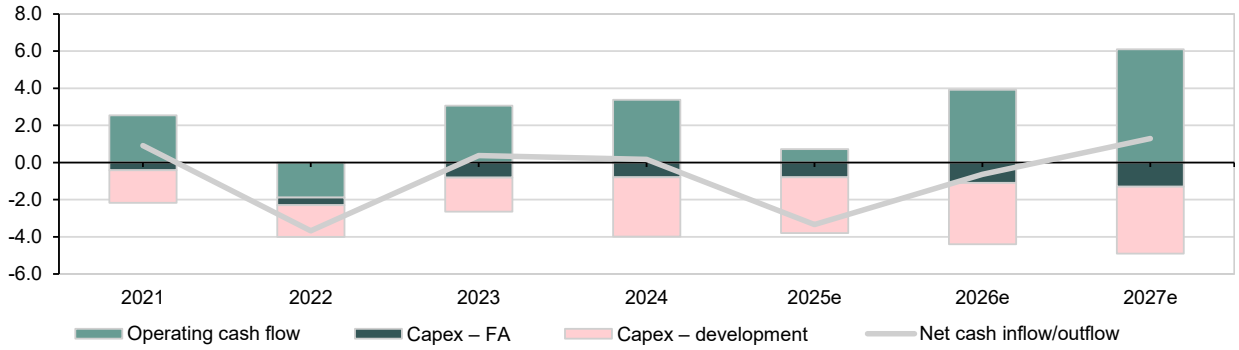
$(000)	2024	2025e	2026e	2027e
Sales	24,559	24,700	28,700	33,500
Growth	9.9%	0.6%	16.2%	16.7%
Adjusted EBITDA	2,984	(152)	2,727	4,858
Growth	49.9%	-105.1%	-1887.9%	78.2%
Margin	12.2%	-0.6%	9.5%	14.5%
Adjusted EBIT	1,039	(2,283)	327	2,168
Growth	n/a	-319.7%	-114.3%	563.9%
Margin	4.2%	-9.2%	1.1%	6.5%
Adjusted diluted EPS ($)	0.16	(0.33)	0.05	0.32
Growth	n/a	-214.6%	-14.3%	663.9%
Operating Cash Flow	3,315	661	3,823	5,947
Free Cash Flow	(664)	(3,139)	(577)	1,047
Year-end net Debt/(Cash)	(5,321)	(2,336)	(1,699)	(2,994)

Source: Edison Investment Research

Cash generation and balance sheet

We expect to see a net cash outflow in the current year (Exhibit 23), resulting in year-end net cash of $2.3m. As operating profitability improves with revenue expansion, operating cash flows strongly increase as indicated. Management highlighted on the H125 results conference call an expectation that the business will be net cash flow positive from H226, and we expect significant net cash generation in 2027e. Over the forecast period, we expect Corero to remain in a net cash position, with our forecasts allowing for continued capital investment to support new product initiatives.

Exhibit 19: Operating and free cash flow ($m), 2021–27e



Source: Edison Investment Research

Valuation

The challenges associated with valuing smaller technology businesses operating at the leading edge of their particular technology 'domain' are long-established. With a relatively small current share of the addressable market opportunity, Corero's application of innovative technology and recently enhanced sales channels should ensure a long-term growth trajectory and margin upside, which, by its very nature, is hard to capture in the near-term time horizon of our forecasts.

Moreover, while we fully expect that the business can achieve our targets as a standalone entity under the guidance of the new CEO, we note the high level of consolidation in recent years, specifically among vendors of cybersecurity solutions. This reflects the structural long-term growth drivers of this industry segment: we are in an era of ongoing 'digital transformation' across most industries, in which cybersecurity is a clear imperative. Recent high-profile cyberattacks such as those on Jaguar Land Rover, Marks & Spencer, Adidas, Gucci, Harrods and Co-op have illustrated the challenge.

We assess Corero's value in several ways. We compare its current valuation based on industry peers using our conservative near-term projections. However, we feel more weight should be given to a valuation based on longer projections, specifically based on the cash flow generation as the business scales. This latter method implies impressive upside.

Industry peer multiples

In the table below, we show Corero's current valuation metrics, together with those of the peer group of leading cybersecurity businesses. As shown, the metrics based on nearer-term profitability show Corero's premium to peers, albeit with that premium reducing rapidly over the forecast period. This principally reflects the fact that Corero, with its innovative application of technology to DDoS, is less 'mature' than many of these businesses and, from a smaller revenue base, can be expected to see margins expand more rapidly.

This point is emphasised by the fact that when we look at the EV/sales metric or the value that the market is applying to the sales 'franchise' of the business, Corero appears markedly undervalued (by c 60%) against the average of the peer group.

Exhibit 20: Peer group valuation comparisons

		Reporting	Price	Market cap	EV	EV/sales (x)			EV/EBITDA (x)			P/E (x)		
	Year-end	currency	(in reporting currency)			Yr 1	Yr 2	Yr 3	Yr 1	Yr 2	Yr 3	Yr 1	Yr 2	Yr 3
A10 Networks	Dec	USD	18	1,275	1,126	4.0	3.7	3.4	14.0	12.8	12.3	20.4	18.2	0.0
Check Point Software Technologies	Dec	USD	199	21,617	20,148	7.4	7.0	6.6	17.4	16.6	15.4	18.0	18.9	17.2
CyberArk Software	Dec	USD	398	26,070	25,750	19.3	16.2	13.6	86.3	66.1	54.3	133.2	106.4	80.0
Fastly	Dec	USD	8	1,176	1,193	2.0	1.9	1.8	25.0	18.9	13.5	n/a	n/a	n/a
F5	Sept	USD	301	14,807	13,463	4.3	4.1	4.0	11.7	11.0	11.0	17.1	15.8	15.0
PagerDuty	Jan	USD	16	1,469	1,312	2.6	2.5	2.3	10.4	9.2	8.4	15.2	13.8	11.8
Palo Alto Networks	July	USD	218	147,741	144,837	13.8	12.1	10.9	43.3	38.3	33.5	57.2	50.7	44.5
OneSpan	Dec	USD	16	594	502	2.0	1.9	1.8	6.8	6.4	6.0	10.9	10.5	10.1
Radware	Dec	USD	25	1,084	884	2.9	2.7	2.5	18.0	16.7	13.0	22.4	21.5	19.2
Trend Micro	Dec	JPY	7,883	7,207	5,839	3.3	3.2	3.0	11.0	10.5	9.5	30.5	24.6	21.9
Average						**6.2**	**5.5**	**5.0**	**24.4**	**20.7**	**17.7**	**36.1**	**31.2**	**24.4**
Corero Network Security	Dec	USD	13	66	62	2.4	2.0	1.7	n/r	21.4	12.0	n/m	n/m	40.0
Corero premium/(discount)						-61%	-64%	-66%	n/r	4%	-32%	n/m	n/m	64%

Source: LSEG Data & Analytics, Edison Investment Research. Note: Prices as at 5 November.

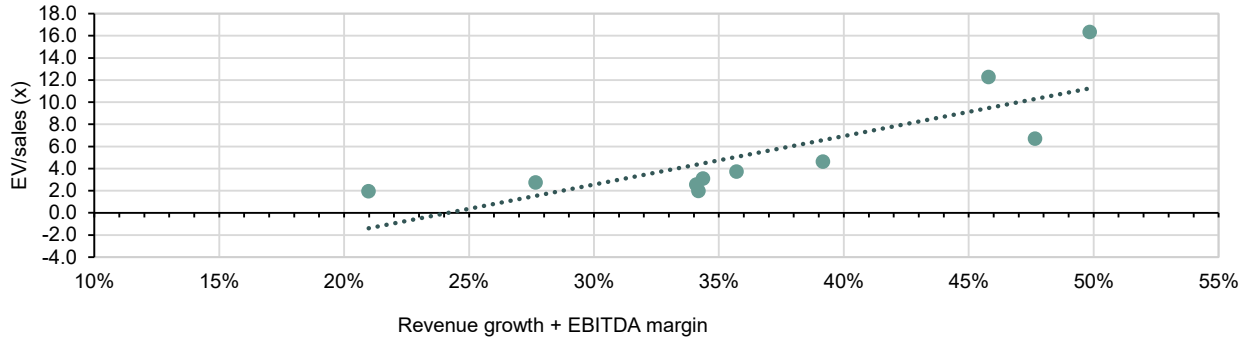
Applying the Rule of 40

Benchmarking using the Rule of 40 is also, we believe, an appropriate tool to use when assessing the value of Corero relative to its peers. The Rule of 40 is useful for faster-growth, SaaS-based business models and helps assess how a business is balancing its profitability with growth. It is also a useful way to benchmark businesses that may be at different stages of development and with a different operating (cost) structure to reflect their various states of maturity along the business cycle.

The Rule of 40 principle is that a SaaS-based business should be able to operate with a combined growth rate and profit margin of 40% or more. For example, a business operating with 30% growth should be able to command margins of 10% and a business with slower growth of 10% should be able to achieve margins of 30%. We note that Corero's ARR growth in H125 of 25% and our expectation of a mid-term EBITDA margin of 15% (2027e) are strong indicators that the company has the potential to justify being viewed under the Rule of 40 benchmark.

The value in applying the Rule of 40 to a group of businesses is that we can assess how, relative to its peers, Corero is valued when normalising for its different level of maturity. In the chart below, the regression line has the equation: EV/sales = 43 x (revenue growth + EBITDA margin) - 10. From this we can calculate Corero's implied market cap and share price, which are $88m (£66m) and $0.17 (13p), respectively, suggesting share price upside of 35%.

Exhibit 21: Rule of 40 regression analysis

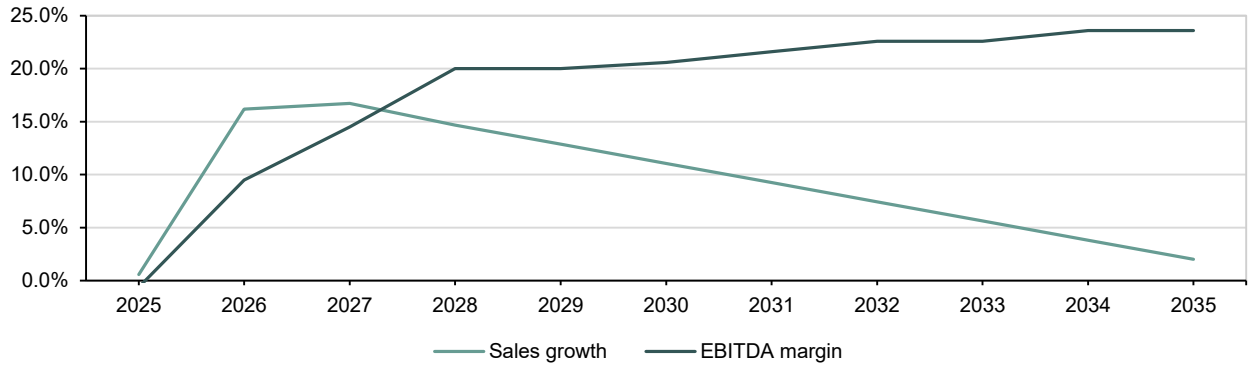


Source: Edison Investment Research

Longer-term DCF valuation

Given the longer-term structural drivers of demand and, as discussed, the expected improvement in free cash flow, a better way to assess Corero's longer-term value may be achieved by looking at the implied fair value of the equity by using DCF modelling. The key inputs to the model of revenue growth and margin expansion over the 10-year period are summarised below. We note the conservative assumptions that a) revenue growth tapers beyond the current forecast period such that in year 10 (2035) growth is at the assumed terminal growth rate, and b) EBITDA margins peak at just 22.5% (in 2032) where they remain.

Exhibit 22: Input assumptions for DCF modelling



Source: Edison Investment Research

Clearly, such modelling is not without challenges, not least choosing an appropriate weighted average cost of capital (WACC) to apply in discounting forecast cash flows. Using the current 10-year UK gilt (4.5%) as the risk-free rate, the UK market risk premium of 5.1% (source: Damodaran, Stern School of Business, New York University), together with Corero's beta of 0.2 implies a WACC of 5.5%. However, the beta of 0.2 is arguably 'understated' and suppressed somewhat by the lower equity liquidity. A beta of 1.0 (implying volatility in line with the UK market) would suggest a WACC of 9.6%. In reality, a more appropriate WACC is somewhere between the two figures.

Therefore, a sensible approach to assessing the implied fair value of the equity is to look at its sensitivity as a function of the WACC and the assumed terminal growth rate, which we show below. As highlighted, more conservative assumptions on WACC as well as terminal growth suggest a fair value of $0.22 (17p) per share, which is 76% upside to the current share price.

Exhibit 23: DCF implied fair equity value sensitivity analysis ($/share)

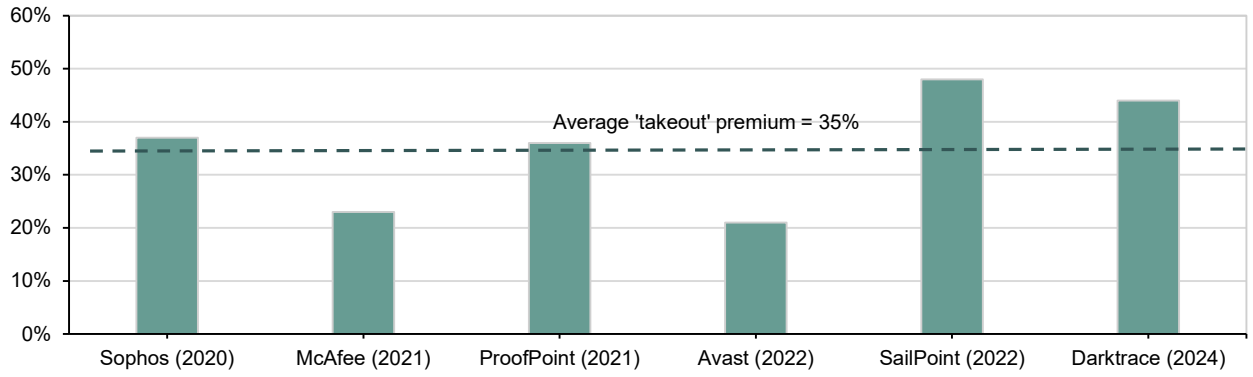
		Terminal growth						
		1.875%	2.000%	2.125%	2.250%	2.375%	2.500%	2.625%
WACC	4.50%	0.52	0.55	0.58	0.61	0.65	0.69	0.74
	5.00%	0.43	0.45	0.47	0.49	0.51	0.54	0.56
	5.50%	0.36	0.37	0.39	0.40	0.42	0.43	0.45
	6.00%	0.31	0.32	0.33	0.34	0.35	0.36	0.38
	6.50%	0.27	0.27	0.28	0.29	0.30	0.31	0.32
	7.00%	0.23	0.24	0.25	0.25	0.26	0.27	0.27
	7.50%	0.21	0.21	0.22	0.22	0.23	0.23	0.24
	8.00%	0.19	0.19	0.19	0.20	0.20	0.21	0.21
	8.50%	0.17	0.17	0.17	0.18	0.18	0.18	0.19
	9.00%	0.15	0.15	0.16	0.16	0.16	0.17	0.17
	9.50%	0.14	0.14	0.14	0.15	0.15	0.15	0.15
	10.00%	0.13	0.13	0.13	0.13	0.13	0.14	0.14
	10.50%	0.12	0.12	0.12	0.12	0.12	0.13	0.13

Source: Edison Investment Research

Industry consolidation and take out premiums

While we fully expect management to deliver on its strategic targets of growth, market share gains and steady increases in profitability as a standalone business, it is important to note the high degree of consolidation seen in the cybersecurity technology sector. Many of the purchases made in the last five years have been of smaller private businesses and so establishing any 'takeout' premium is extremely hard. However, the process is ongoing at both ends of the consolidation scale, as evidenced by Cyberfort's recent purchase of ZDL in the UK, as well as the much larger transaction in which Alphabet agreed to purchase Israel-based Wiz. The chart below demonstrates the level of takeout premium where publicly listed cybersecurity businesses have been consolidated.

Exhibit 24: Takeout premium of listed cybersecurity businesses 2020–25



Source: Edison Investment Research

Exhibit 25: Financial summary

$000s	2022	2023	2024	2025e	2026e	2027e
Year end 31 December	IFRS	IFRS	IFRS	IFRS	IFRS	IFRS
INCOME STATEMENT						
Revenue	20,121	22,349	24,559	24,700	28,700	33,500
Other income	0	0	0	0	0	0
Total output	20,121	22,349	24,559	24,700	28,700	33,500
Cost of Sales	(2,576)	(2,164)	(2,134)	(2,149)	(2,440)	(2,848)
Gross Profit	17,545	20,185	22,425	22,551	26,261	30,653
EBITDA	3,375	1,990	2,984	(152)	2,727	4,858
Reported EBITDA	2,619	1,757	2,500	(449)	2,153	4,188
Operating profit (before amort. and excepts.)	1,062	217	976	(2,353)	227	2,008
Share-based payments	(386)	(233)	(484)	(296)	(574)	(670)
Reported operating profit	676	(16)	492	(2,649)	(348)	1,338
Net Interest	(272)	(137)	63	70	100	160
Profit Before Tax (norm)	790	80	1,039	(2,283)	327	2,168
Profit Before Tax (reported)	404	(153)	555	(2,579)	(248)	1,498
Reported tax	150	(17)	(56)	645	62	(374)
Profit After Tax (norm)	593	60	779	(1,712)	245	1,626
Profit After Tax (reported)	554	(170)	499	(1,934)	(186)	1,123
Net income (normalised)	593	60	779	(1,712)	245	1,626
Net income (reported)	554	(170)	499	(1,934)	(186)	1,123
Average Number of Shares Outstanding (m)	496	500	500	512	512	512
EPS - basic normalised (c)	0.12	0.01	0.16	(0.33)	0.05	0.32
EPS - normalised fully diluted (c)	0.12	0.01	0.16	(0.33)	0.05	0.32
EPS - basic reported (c)	0.11	(0.03)	0.10	(0.38)	(0.04)	0.22
Dividend (c)	0	0	0	0	0	0
BALANCE SHEET						
Fixed Assets	14,159	14,753	16,496	18,232	20,157	22,257
Intangible Assets	13,493	13,811	15,413	16,713	18,113	19,563
Tangible Assets	604	633	944	1,244	1,744	2,344
Investments & other	62	309	139	275	300	350
Current Assets	12,675	13,683	17,000	14,786	15,949	19,044
Stocks	164	96	389	450	500	550
Debtors	6,865	8,427	11,290	12,000	13,750	15,500
Cash & cash equivalents	5,646	5,160	5,321	2,336	1,699	2,994
Other	0	0	0	0	0	0
Current Liabilities	(8,328)	(9,058)	(11,303)	(12,140)	(14,098)	(16,440)
Creditors	(3,956)	(3,902)	(4,340)	(4,470)	(5,100)	(5,750)
Tax and social security	0	0	0	0	0	0
Short-term borrowings	(971)	0	0	0	0	0
Lease liabilities	(78)	(164)	(102)	(170)	(198)	(225)
Other	(3,323)	(4,992)	(6,861)	(7,500)	(8,800)	(10,465)
Long-Term Liabilities	(2,522)	(2,642)	(3,529)	(4,169)	(5,285)	(6,815)
Long-term borrowings	(237)	0	0	0	0	0
Lease liabilities	0	(151)	(48)	(170)	(190)	(215)
Other long-term liabilities	(2,285)	(2,491)	(3,481)	(3,999)	(5,095)	(6,600)
Net Assets	15,984	16,736	18,664	16,709	16,723	18,046
Minority interests	0	0	0	0	0	0
Shareholders' equity	15,984	16,736	18,664	16,709	16,723	18,046
CASH FLOW						
Operating Cash Flow	2,497	1,603	2,507	266	2,314	3,973
Working capital	(5,254)	855	131	100	800	1,100
Exceptional & other	878	659	694	(188)	662	1,154
Tax	150	(17)	(17)	484	46	(281)
Net operating cash flow	(1,729)	3,100	3,315	661	3,823	5,947
Capex	(2,124)	(2,636)	(3,979)	(3,800)	(4,400)	(4,900)
Acquisitions/disposals	0	0	0	0	0	0
Net interest	(151)	(34)	63	70	100	160
Equity financing	228	165	994	0	0	0
Borrowings	0	0	0	0	0	0
Dividends	0	0	0	0	0	0
Other	101	(222)	(222)	(265)	(160)	88
Net Cash Flow	(3,675)	373	171	(3,334)	(637)	1,295
Opening net debt/(cash)	(8,424)	(4,438)	(5,160)	(5,321)	(2,336)	(1,699)
FX	(311)	349	(10)	349	0	0
Other non-cash movements	0	0	0	0	0	0
Closing net debt/(cash)	(4,438)	(5,160)	(5,321)	(2,336)	(1,699)	(2,994)

Source: Company accounts, Edison Investment Research

Appendix

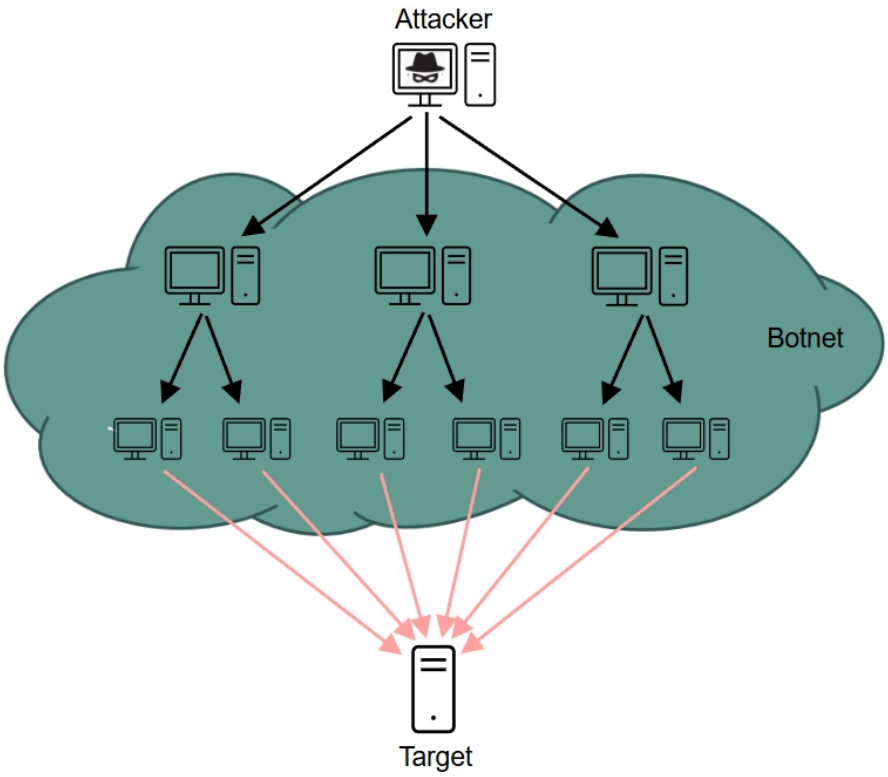
The DDoS problem

A DDoS attack is a cyberattack on a website, online service, specific network or a computer that results in that service being taken offline, by flooding the target with a very high quantity of 'requests' such that the target cannot cope. The concept is a fairly unsophisticated mechanism to cause service failure, but over time the methods deployed by the perpetrators of the attacks have become more sophisticated and therefore companies require increasingly more sophisticated solutions for protection.

Early denial of service (DoS) attacks used a single point of access or internet connection to barrage a target with fake requests. In contrast, a DDoS attack uses multiple points of internet access (even millions) to create high volumes of data traffic. This can be carried out in a number of ways, but most commonly involves the use of botnets.

Botnets are created when a hacker is able to hack into a device (any device with an internet connection) and insert a malicious piece of code or malware, termed a 'bot'. In contrast to the more commonly known 'chatbots' used to automate decision-making or direct online queries on a website, malicious bots are orchestrated to act together in a botnet. The botnet can then be instructed to flood a target's servers and devices with a high volume of requests.

Exhibit 26: DDoS attack perpetration



Source: Edison Investment Research

This rise in the level of attack sophistication reflects the type of attacker and their motivation. Early DDoS attacks tended to be driven by individuals, typically using open-source tools to generate and direct traffic volumes to a particular site. The motivation for the attack might be a personal grievance (as basic as anger at a new game feature), or possibly even just a challenge or 'sport'.

Over time, however, the growth of hacktivism has materially changed the identities of the threat attackers and the resources available to them. Threat attackers now increasingly include large, organised online organisations motivated by the potential to make significant financial gain. In many instances, state-sponsored organisations undertake DDoS

attacks with the specific aim of harming the commercial and state infrastructure of other nations.

In recent years, there has been a commoditising of DDoS attacks, which has helped them to become increasingly prevalent and more damaging. For example, services now exist that allow anyone to launch a DDoS attack without having to create their own botnet. These readily available services are known as DDoS-for-hire or DDoS as a service and provide attackers with the capability to launch powerful DDoS attacks without any technical expertise.

Types of DDoS attack

While there are myriad DDoS attack threat types or 'vectors', the threat landscape can be broadly divided into those that have an impact in one of two ways, best categorised with reference to the Open Systems Interconnection (OSI) model of how network protocols are organised:

- **Layer 3/Layer 4 attacks:** affecting the wider cloud infrastructure, typically (although not exclusively) having an impact by exhausting the resources of network infrastructure, meaning that legitimate users cannot access the service. These types of attack are a particular nuisance to telecommunication and internet service providers (ISPs).
- **Layer 7 attacks:** affecting primarily the corporate level, application layer attacks target the performance of web applications and on-premise located services and solutions that have an interface with cloud/online services.

Exhibit 27: Types of DDoS attack

OSI layer	Key functional role	DDoS attack threats / vectors
7 – Application layer	Human-computer interaction layer where applications access the network services	DNS query attacks, HTTP Floods, Zero-day, Slowloris, buffer overflow, SQL Injection, cookie poisoning
6 – Presentation layer	Ensures that data is in a usable format and is where data encryption occurs	No attacks at this level
5 – Session layer	Maintains connections and is responsible for controlling ports and session	SSL renegotiation, MITM attacks, session token hijacking, Telnet exploits (mainly obsolete)
4 – Transport layer	Transmits data using transmission protocols (eg TCP and UDP)	SYN Floods, ACK Floods, Smurf attacks, Ping of Death
3 – Network layer	Defines the physical path the data will take	UDP reflection attacks, amplification attacks, Ping of Death, IP Spoofing ICMP Echo
2 – Datalink layer	Defines the format of data on the network	No attacks at this level
1 – Physical layer	Transmits raw data bit stream over the physical medium	No attacks at this level

Source: Edison Investment Research, the Open Systems Interconnection model

In reality, few corporates are run using entirely cloud-based or entirely on-premise IT solutions; most essentially run a hybrid IT model.

Perpetrators of DDoS attacks

In addition to attacks predominantly driven by financial gain, the DDoS attack industry is also a consequence of DDoS being a popular tool of state-sponsored attackers. For example, in the current conflict between Russia and Ukraine, DDoS attacks have played an important role and are used as a low-cost method of disruption by hacktivists.

Organised groups that are effectively 'for hire' to propagate DDoS attacks include:

- **KillNet:** a pro-Russian hacktivist group, which, apart from targeting Ukraine, has frequently targeted other NATO countries, governments and critical infrastructure.
- **Anonymous Sudan:** believed to be a Russia-based group that has propagated a series of politically motivated attacks.
- **Lazarus Group:** a group sponsored by the North Korean state, known to have undertaken a number of international cyberattacks, including DDoS.

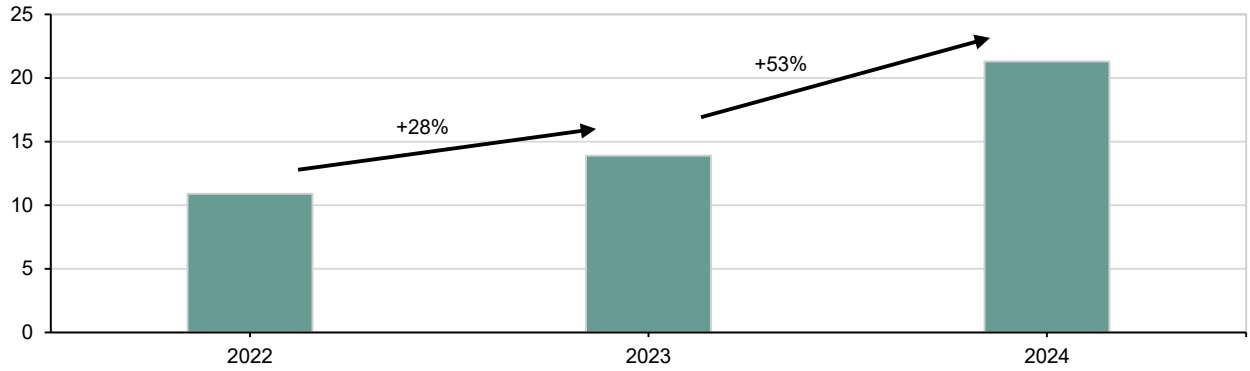
- **NoName057(16):** a pro-Russian hacking group that has claimed responsibility for cyberattacks on US and European government agencies since early 2022.
- **DragonForce Malaysia:** a pro-Palestinian hacktivist group based in Malaysia, which has targeted government agencies and organisations across the Middle East and Asia.

A growing problem

The true extent of DDoS attacks is hard to assess. For obvious reasons, the majority of businesses prefer not to state or publicise data on the extent to which they have been the subject of attacks. In reality, the world gets to hear of attacks when they are successful and cause disruption or occasionally when providers of DDoS services publicise successful mitigation against increasingly larger and aggressive forms of attack.

In 2019, Cisco Systems' Annual Internet Report concluded that it expected the number of DDoS attacks globally to double from 7.9m in 2018 to 15.4m in 2023. In hindsight, this appears to have been a material under-assessment of the size of the risk, implying a CAGR over the period of 14%. Most providers of DDoS detection and mitigation services have cited materially faster growth in recent years. As an example, Cloudflare, which claims to provide DDoS protection services to around 18,000 customers, has published data in which it estimates that the business has seen a doubling in attacks over 2022–24 alone (see exhibit below). Moreover, taking into consideration Cloudflare's claim that its services cover around 20% of websites, the implication is that globally the number of attacks in 2024 was actually closer to 100m.

Exhibit 28: Growth in DDoS attacks globally (2022–24), millions

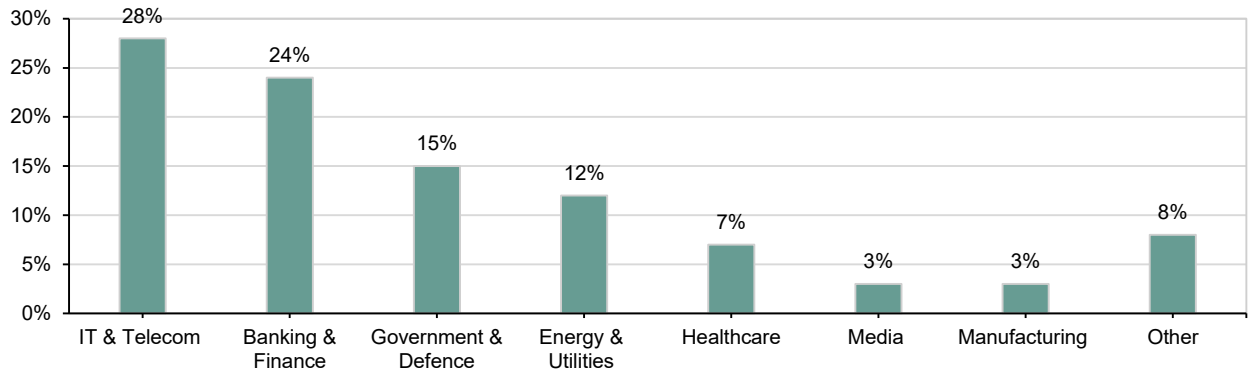


Source: Cloudflare data, Edison Investment Research. Note: Chart shows Cloudflare's disclosed detection of customer attacks.

The acceleration in attacks in 2024 is corroborated by data published by many industry players. Apart from obvious increasing geopolitical tensions (and an increase in the number of state-sponsored attacks), another key driver of this trend is the proliferation of poorly secured IoT devices, which has facilitated the ease with which attackers have been able to create the botnets and scale their attacks.

Exhibit 4 shows the profile by end-user industry segment of where attacks were focused. Somewhat predictably, attacks targeted at telecoms providers, banking and finance and government (including defence) entities collectively make up two-thirds of all attack volumes.

Exhibit 29: DDoS attack profile by end-user industry

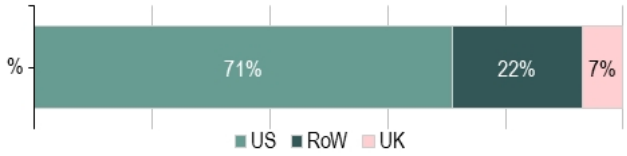


Source: Aggregated industry data, Edison Investment Research

Contact details

US headquarters:
293 Boston Post Road West
Suite 310
Marlborough MA 01752
+ 1 978 212 1500
EMEA headquarters:
Salisbury House
29 Finsbury Circus
London EC2M 5QQ
+44 1895 876382
www.corero.com

Revenue by geography



Management team

CEO: Carl Herberger

Appointed to the board in January 2024, Carl brings over 25 years of cybersecurity leadership experience. As an internationally recognised expert, he has held executive roles at top security firms including Radware, Evolve IP, Allied InfoSecurity and most recently as principal security consultant and virtual CISO. Among his many achievements, Carl received the Technology Executive of the Year award in 2019 and helped establish the US Air Force's first cyber warfare unit during his time as an intelligence officer. As CEO, he leverages his deep expertise across all facets of cybersecurity to lead Corero's corporate strategy and help its customers manage risk and build resilient systems capable of withstanding today's cyber threats.

CFO: Chris Goulden

Chris joined Corero in May 2024 after 12 years at CBRE, where he held a number of senior positions including finance director of the UK and, more recently, finance director for the Central Europe and Nordics regions. Prior to this, Chris held a number of roles over a period of three years at BNP Paribas. He qualified as an accountant with Ernst & Young.

Non-executive chairman: Jens Montanana

Jens has spent the majority of his over 30-year career in the technology industry, with considerable operational and commercial experience in the resale and distribution of information technology hardware and software solutions. He is the founder and CEO of Datatec, which was established in 1986 and listed on the Johannesburg Stock Exchange in 1994. Between 1989 and 1993 Jens served as MD and VP of US Robotics (UK), a wholly owned subsidiary of US Robotics, which was acquired by 3Com. In 1993, he co-founded US start-up Xedia Corporation in Boston, an early pioneer of network switching and IP bandwidth management, which was subsequently sold to Lucent Corporation in 1999 for $246m. Jens has served on the boards and sub-committees of various public companies.

Independent non-executive director: Peter George

Peter has a successful track record as CEO of leading IT network and security companies and provides sales and marketing leadership experience to the board. Until late 2024, Peter was the CEO of Evolv Technology, a US-based leader in human security screening. Prior to that he was president and CEO of empow cybersecurity, a market innovator in AI, machine learning and advanced security analytics.

Independent non-executive director: Richard Last

Richard has over 20 years' senior experience in information technology having worked at board level for a number of publicly quoted and private companies in the technology sector. He is a Fellow of the Institute of Chartered Accountants in England and Wales. Richard is a Corero shareholder and has been a non-executive director of the company for over 10 years; his independence has been considered by the board. The board is satisfied that Richard Last operates in an independent manner and is independent. Richard is currently the executive chair at Iomart, a leading provider of cloud managed services.

Non-independent non-executive director: Andrew Miller

Andrew served as Corero's CFO from 2010 to 2019. Until February 2025, he was CFO of Mycom, a telecoms SaaS provider, and prior to that he was CFO and COO of C5 Capital, an investment firm investing in the secure data ecosystem including cybersecurity, cloud infrastructure, data analytics and space, and CFO of the Haven Group, a private equity-backed cybersecurity services provider. Prior to joining Corero, Andrew was with the Datatec group in a number of roles between 2000 and 2009, including operations director of Logicalis Group and director of corporate finance and strategy. Prior to this, Andrew gained considerable corporate finance experience in London with Standard Bank, West Deutsche Landesbank and Coopers & Lybrand. He trained and qualified as a chartered accountant and has a bachelor's degree in commerce from the University of Natal, South Africa. Andrew is a chartered accountant with over 20 years' experience in the technology industry.

Principal shareholders

	%
Jens Montanana	36.6
Sabvest Capital Holdings	11.2
Caraway Group	10.5
Juniper Networks	9.6
Herald Investment Trust	8.7
Charles Stanley Private Clients	4.2
Peter Kennedy Gain	3.2

General disclaimer and copyright

This report has been commissioned by Corero Network Security and prepared and issued by Edison, in consideration of a fee payable by Corero Network Security. Edison Investment Research standard fees are £60,000 pa for the production and broad dissemination of a detailed note (Outlook) following by regular (typically quarterly) update notes. Fees are paid upfront in cash without recourse. Edison may seek additional fees for the provision of roadshows and related IR services for the client but does not get remunerated for any investment banking services. We never take payment in stock, options or warrants for any of our services.

Accuracy of content: All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable, however we do not guarantee the accuracy or completeness of this report and have not sought for this information to be independently verified. Opinions contained in this report represent those of the research department of Edison at the time of publication. Forward-looking information or statements in this report contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations.

Exclusion of Liability: To the fullest extent allowed by law, Edison shall not be liable for any direct, indirect or consequential losses, loss of profits, damages, costs or expenses incurred or suffered by you arising out or in connection with the access to, use of or reliance on any information contained on this note.

No personalised advice: The information that we provide should not be construed in any manner whatsoever as, personalised advice. Also, the information provided by us should not be construed by any subscriber or prospective subscriber as Edison's solicitation to effect, or attempt to effect, any transaction in a security. The securities described in the report may not be eligible for sale in all jurisdictions or to certain categories of investors.

Investment in securities mentioned: Edison has a restrictive policy relating to personal dealing and conflicts of interest. Edison Group does not conduct any investment business and, accordingly, does not itself hold any positions in the securities mentioned in this report. However, the respective directors, officers, employees and contractors of Edison may have a position in any or related securities mentioned in this report, subject to Edison's policies on personal dealing and conflicts of interest.

Australia

Edison Investment Research Pty Ltd (Edison AU) is the Australian subsidiary of Edison. Edison AU is a Corporate Authorised Representative (1252501) of Crown Wealth Group Pty Ltd who holds an Australian Financial Services Licence (Number: 494274). This research is issued in Australia by Edison AU and any access to it, is intended only for "wholesale clients" within the meaning of the Corporations Act 2001 of Australia. Any advice given by Edison AU is general advice only and does not take into account your personal circumstances, needs or objectives. You should, before acting on this advice, consider the appropriateness of the advice, having regard to your objectives, financial situation and needs. If our advice relates to the acquisition, or possible acquisition, of a particular financial product you should read any relevant Product Disclosure Statement or like instrument.

New Zealand

The research in this document is intended for New Zealand resident professional financial advisers or brokers (for use in their roles as financial advisers or brokers) and habitual investors who are "wholesale clients" for the purpose of the Financial Advisers Act 2008 (FAA) (as described in sections 5(c) (1)(a), (b) and (c) of the FAA). This is not a solicitation or inducement to buy, sell, subscribe, or underwrite any securities mentioned or in the topic of this document. For the purpose of the FAA, the content of this report is of a general nature, is intended as a source of general information only and is not intended to constitute a recommendation or opinion in relation to acquiring or disposing (including refraining from acquiring or disposing) of securities. The distribution of this document is not a "personalised service" and, to the extent that it contains any financial advice, is intended only as a "class service" provided by Edison within the meaning of the FAA (i.e. without taking into account the particular financial situation or goals of any person). As such, it should not be relied upon in making an investment decision.

United Kingdom

This document is prepared and provided by Edison for information purposes only and should not be construed as an offer or sol icitation for investment in any securities mentioned or in the topic of this document. A marketing communication under FCA Rules, this document has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research.

This Communication is being distributed in the United Kingdom and is directed only at (i) persons having professional experience in matters relating to investments, i.e. investment professionals within the meaning of Article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005, as amended (the "FPO") (ii) high net-worth companies, unincorporated associations or other bodies within the meaning of Article 49 of the FPO and (iii) persons to whom it is otherwise lawful to distribute it. The investment or investment activity to which this document relates is available only to such persons. It is not intended that this document be distributed or passed on, directly or indirectly, to any other class of persons and in any event and under no circumstances should persons of any other description rely on or act upon the contents of this document.

This Communication is being supplied to you solely for your information and may not be reproduced by, further distributed to or published in whole or in part by, any other person.

United States

Edison relies upon the "publishers' exclusion" from the definition of investment adviser under Section 202(a)(11) of the Investment Advisers Act of 1940 and corresponding state securities laws. This report is a bona fide publication of general and regular circulation offering impersonal investment-related advice, not tailored to a specific investment portfolio or the needs of current and/or prospective subscribers. As such, Edison does not offer or provide personal advice and the research provided is for informational purposes only. No mention of a particular security in this report constitutes a recommendation to buy, sell or hold that or any security, or that any particular security, portfolio of securities, transaction or investment strategy is suitable for any specific person.

London | New York | Frankfurt
20 Red Lion Street
London, WC1R 4PS
United Kingdom