Clavister

Reason: Initiating coverage

Security by Sweden

- Protecting 5G networks and government agencies
- En route to achieving positive EBITDA in 2022
- Initiating coverage with a fair value range of SEK 5-16

Major potential, but it has struggled with execution

Media reports about critical infrastructure such as hospitals and businesses being paralysed for days by hackers are becoming increasingly common. The total economic damage from cybercrimes is expected to reach USD 6tn in '21, or 40x total cybersecurity spending. Clavister is a Swedish cybersecurity firm that helps keep critical government agencies, enterprises and 5G networks safe. Despite its small size, it is well positioned as a leading European vendor to capitalise on a growing market and to fend off large US multinationals in light of mounting geopolitical tensions and EU privacy regulations. We believe that Clavister will outgrow the market, which Gartner expects to expand at 12% p.a. The main growth driver will be the 5G roll-out, where Clavister already works with ~5% of all operators globally. Since its IPO in 2014, it has been struggling with major losses and poor strategic execution. But we see light at the end of the tunnel, due to the growth potential and the company's relatively fixed cost base.

New strategy since 2018 has delivered results

Since 2018, Clavister has implemented a new strategy that has made its offering clearer to clients, while streamlining the sales organisation to focus on its core customer segments: service providers, governments and defence contractors. It is now banking on being able to leverage its relationships with partners to drive the necessary growth to scale. So far, the strategy is working. All incremental sales since 2017 have fallen to the bottom line. If the company can continue growing sales at a ~20% CAGR while keeping costs flat, we see it generating positive EBITDA in '22e and EBIT in '23e. We forecast a 19% sales CAGR '21e-'23e, just shy of its growth ambition of 20% p.a. In terms of EBITDA margin, we forecast 3% and 16% for '22e-'23e, respectively.

We initiate coverage with a fair value range of SEK 5-16

We arrive at a fair value range of SEK 5-16 per share by constructing a DCF and looking at peer multiples. On our estimates, the stock trades at 3.3x '23e EV/sales, compared to the avg. cybersecurity peer of 10.6x.

Analyst(s): simon.jonsson@abgsc.se, +46 8 566 286 84
simon.granath@abgsc.se, +46 8 566 286 32

SEKm	2019	2020	2021e	2022e	2023e
Sales	123	129	138	167	197
EBITDA	-39	-19	-16	6	32
EBITDA margin (%)	*-31.7*	*-15.1*	*-11.5*	*3.3*	*16.1*
EBIT adj	-77	-56	-50	-25	1
EBIT adj margin (%)	*-62.4*	*-43.8*	*-36.1*	*-15.3*	*0.6*
Pretax profit	-119	-81	-73	-47	-21
EPS rep	-7.59	-2.08	-1.33	-0.87	-0.38
EPS adj	-7.19	-2.08	-1.33	-0.87	-0.38
Sales growth (%)	*10.1*	*4.6*	*7.1*	*21.0*	*18.0*
EPS growth (%)	*-45.6*	*72.6*	*36.1*	*35.0*	*56.0*

Source: ABG Sundal Collier, Company data

Company sponsored research

Not rated

Share price (SEK)	08/09/2021	6.9
Fair value range (per share)		5-16
IT, Sweden		
CLAV.ST/CLAV SS		
MCap (SEKm)		379
MCap (EURm)		37
Net debt (EURm)		18
No. of shares (m)		54.8
Free float (%)		*89*
Av. daily volume (k)		12
Next event		Q3 report: 10 Nov

Performance

	1m	3m	12m
Absolute (%)	*-15.0*	*-15.6*	*-32.7*

Source: FactSet

	2021e	2022e	2023e
P/E (x)	-5.2	-8.0	-18.2
P/E adj (x)	-5.2	-8.0	-18.2
P/BVPS (x)	-6.23	-3.50	-2.93
EV/EBITDA (x)	-35.7	111.4	20.3
EV/EBIT adj (x)	-11.4	-24.2	581.6
EV/sales (x)	4.11	3.70	3.26
ROE adj (%)	*201.8*	*30.1*	*-0.1*
Dividend yield (%)	*0*	*0*	*0*
FCF yield (%)	*-22.8*	*-10.0*	*-3.2*
Lease adj. FCF yld (%)	*-24.7*	*-11.9*	*-5.1*
Net IB debt/EBITDA	-11.8	42.8	8.3
Lease adj. ND/EBITDA	-7.4	-148.8	10.1

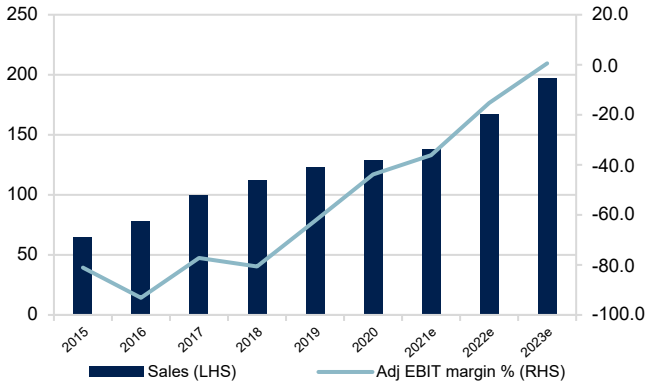
Company description

Clavister develops and sells cybersecurity solutions for physical and virtual environments. Its product portfolio is designed to meet the specific needs of customers in three main categories: public administrations, service providers and defence contractors. Sales are primarily made under the company's own brand, but also through OEMs, i.e. the software being added to the customers' own brands. Clavister has a long list of clients including Nokia, IWG, Telco Systems and BAE Systems.

Risks

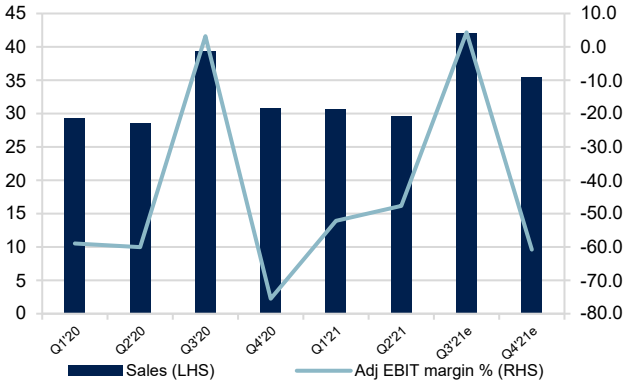
Clavister is dependent on the trust of its customers. If the company's technology does not keep up with current attack methods or meet its customers' expectations, it could lose significant parts of its business. Clavister competes with large multinational corporations, which entails an inherent risk that customers may chose a more well-known vendor over Clavister.

Annual sales and adj. EBIT marginSEKm



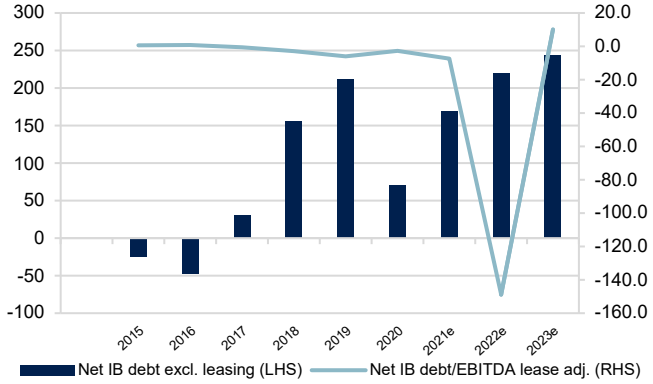
Source: ABG Sundal Collier, Company data

Quarterly sales and adj. EBIT margin



Source: ABG Sundal Collier, Company data

Lease adj. net debt and ND/EBITDA



Source: ABG Sundal Collier, Company data

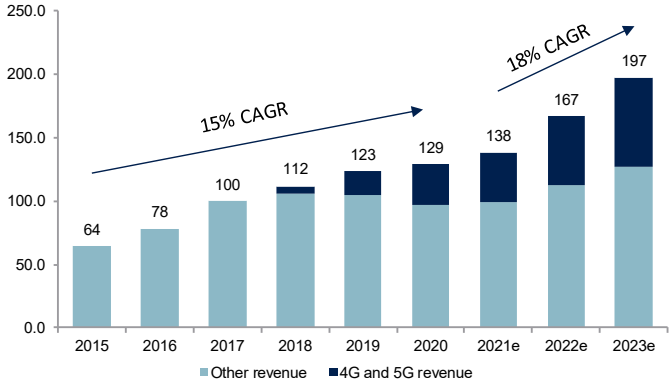
Table of contents

Summary

Clavister is a leading European cybersecurity vendor with over 20 years of experience. The firm is headquartered in Örnsköldsvik (Sweden), with personnel stationed in multiple other locations, including Germany, the UK, Malaysia and other cities in Sweden, such as Stockholm and Gothenburg. Its customers include Communication Service Providers, Governments, Enterprises, and Managed Security Service Providers (MSSPs), in more than 150 countries. We initiate coverage with a fair value range of SEK 5-16 per share. This implies a '22e EV/sales of 3x-7x. We estimate that Clavister will grow its sales by a 19% CAGR from '21e to '23e, and reach positive EBITDA in 2022e.

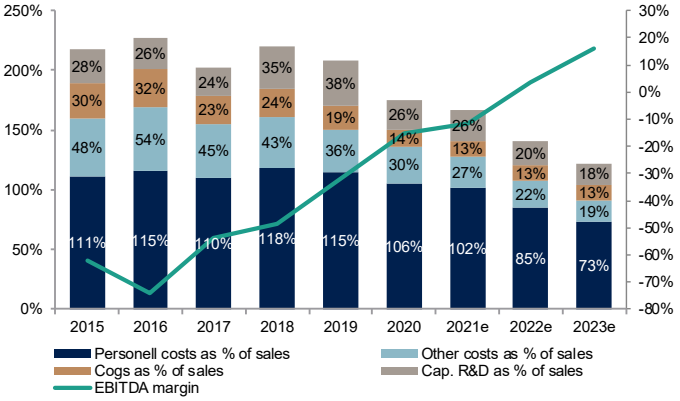
Clavister has traditionally specialised in firewall technology, but started to diversify in 2016 with the acquisition of Identity and Access Management specialist PhenixID. Between 2017 and 2019, the firm embarked on a journey to transition from a single-product supplier to a full cybersecurity solution provider. During that time, it accelerated product development and expanded into virtualised, or cloud-based security. As a result, Clavister now offers competitive solutions for 5G security, enterprise network security, access and authentication, as well as military grade cyber armour. It has managed to attract a solid client list including International Workplace Group (IWG), D-link, Network Equipment Manufacturers like Nokia and many of the critical government agencies in Sweden. The company also collaborates with Intel, ARM, VMware and others.

15% net sales CAGR 2015-2020 (SEKm)



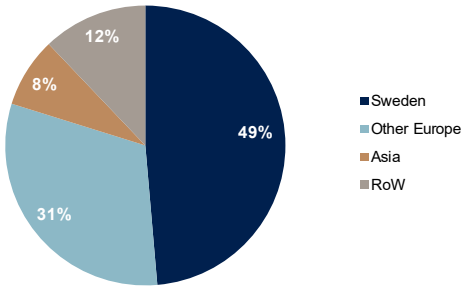
Source: ABG Sundal Collier, company data

Cost items are moving in the right direction



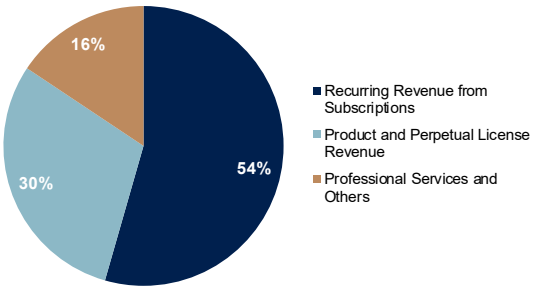
Source: ABG Sundal Collier, company data

Revenue by market, 2020



Source: ABG Sundal Collier, company data

Sales per revenue stream, 2020



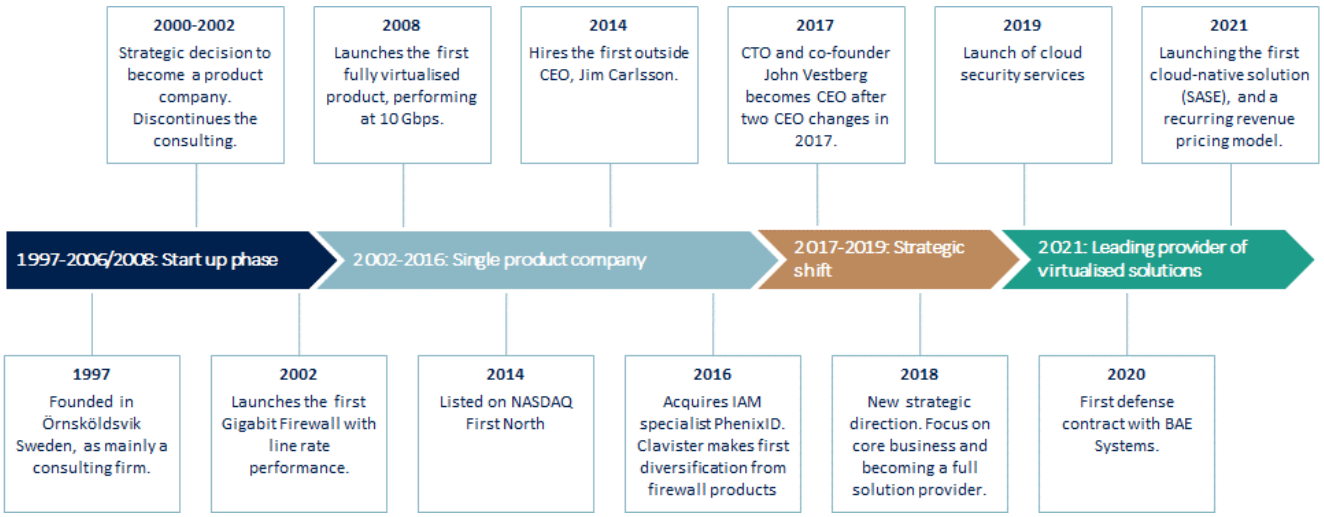
Source: ABG Sundal Collier, company data

History

The Clavister story began in 1997 when two entrepreneurs, Peter Johansson and John Vestberg, joined forces to build a secure router (Vestberg subsequently became CTO and is now CEO). In 2002-2003 the company launched its first hardware appliance, a firewall device that performed well in tests. Around 2006, it started working with OEMs, and signed its first partner deal with D-Link, and the year after with Ericsson.

The first virtual gateway was released in 2008, which marked another critical milestone. At this time, the company started expanding in Europe and later into China (a market that was discontinued in 2019, partly to avoid geopolitical tension). In 2014, the company went public and brought in its first outside CEO. The acquisition of PhenixID in 2016 started a new chapter, and Clavister started developing a broader set of full-scale solutions. Today, the company offers six predefined solutions that cater to specific industry challenges within its three core market segments: Service Providers, EU Public Administration and Defence.

Company timeline

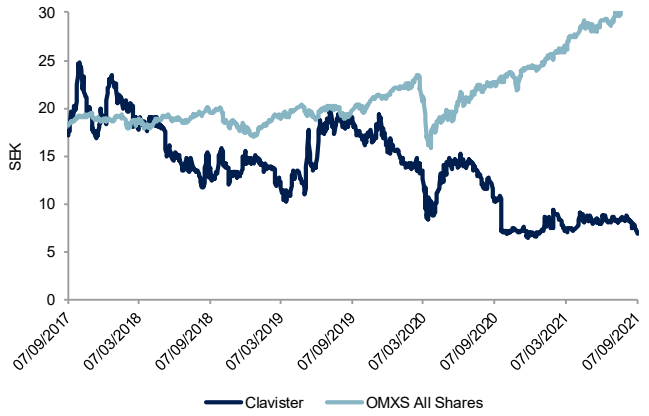


Source: ABG Sundal Collier, company data

Are years of underperformance coming to an end?

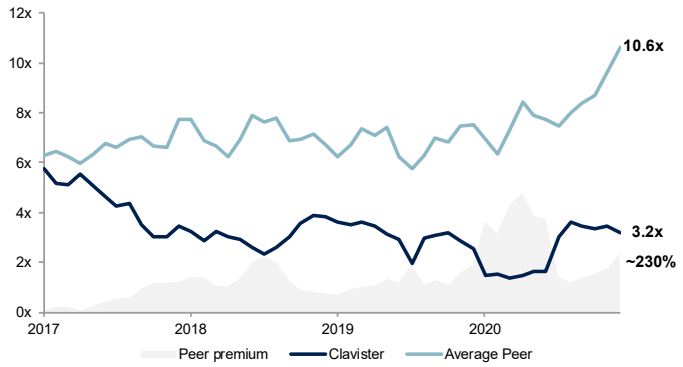
After its IPO in 2014, expectations on the company were set too high. The share topped out at a valuation of ~20x EV/sales in 2015. Since 2017, the share price has declined by ~60%. Today, the share trades at 3.2x (reported) EV/sales, indicating a significant re-rating in expectations. In addition, a significant valuation gap has emerged between Clavister and its peer group.

-60% return in the last four years



Source: ABG Sundal Collier, company data

EV/sales has diverged vs. peers



Source: ABG Sundal Collier, company data

We view the gap in valuation as reasonable given that average profitability among the peer group is very high compared to Clavister, which has been burning cash at a rate of ~SEK 100m p.a. for the last five years. Total FCF in the years from 2017 to 2020 was SEK -370m. We expect that Clavister will continue to burn ~SEK 150m in cash before reaching profitability. This means that while the company raised ~SEK 200m in a 2020 share issue, it could need more external funding before being able to stand on its own.

Competitive technology, but poor execution has hurt performance

Evidence suggests that Clavister's technology is very competitive (more info in the chapter titled *Value proposition*). Still, it remains unprofitable. We attribute this to poor strategic decision making over the years. From its founding in 1997, until 2016 when it acquired the PhenixID IAM business, it essentially offered only one solution. It was not until the implementation of a new strategic direction in 2018 that the company truly started moving towards becoming a multi-solution provider – a necessity if it is to reach sufficient scale.

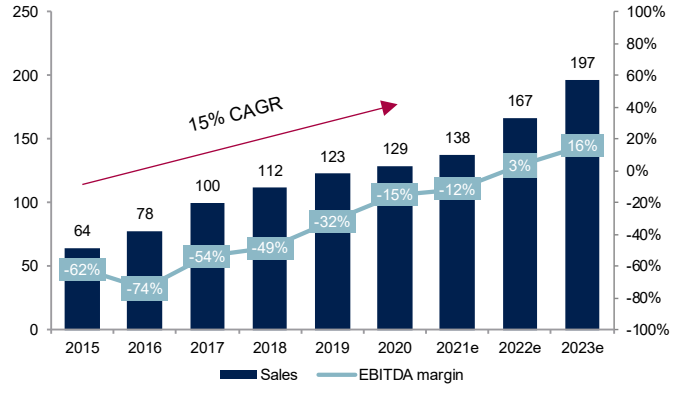
New strategic direction in 2018

The company has used its existing technology platform to build solutions that cater to other security challenges (e.g. leveraging its competence in government agencies by applying it to the defence industry). Additionally, until 2018 the sales and marketing initiatives were highly fragmented. The company had not yet learned or realised what customer segments it should focus its energy on. Now, it has narrowed down its focus to a couple of core market segments where its technology is most competitive (Public Administrations, Service Providers, Defence) and where it believes it can achieve the most scale. Instead of going after enterprises in multiple industries directly – a time- and energy-intensive strategy – it is focusing on strategic partnerships with service providers and system integrators that license or distribute its technology to third-party customers. We view this strategy positively and believe it could generate the sought-after scalability.

New strategy is bearing fruit

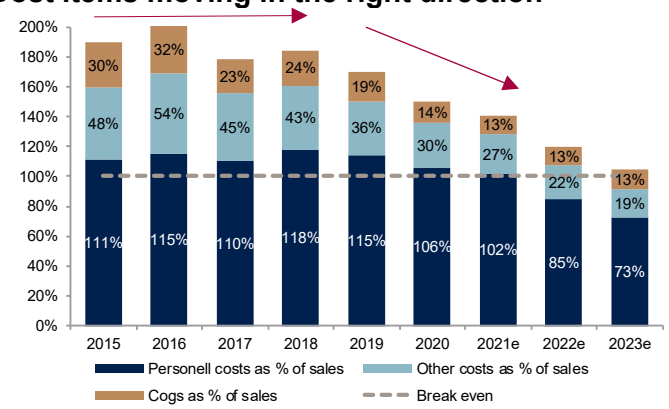
In recent years, the company has been able to attract the interest of several major service providers, including Nokia, Tata Communications and Telco Systems, as well as defence contractors such as BAE Systems. Clavister is essentially able to grow with the partners with low incremental opex requirements. Importantly, we are starting to see this in the numbers as well. Since 2018, operating costs have started to decline in relation to sales, which has had a significant impact on EBITDA. We expect EBITDA to reach positive territory in 2022, almost exclusively driven by top-line growth and significant scalability through a high gross margin (+90%) and low incremental investments.

Sales and EBITDA margins both increasing



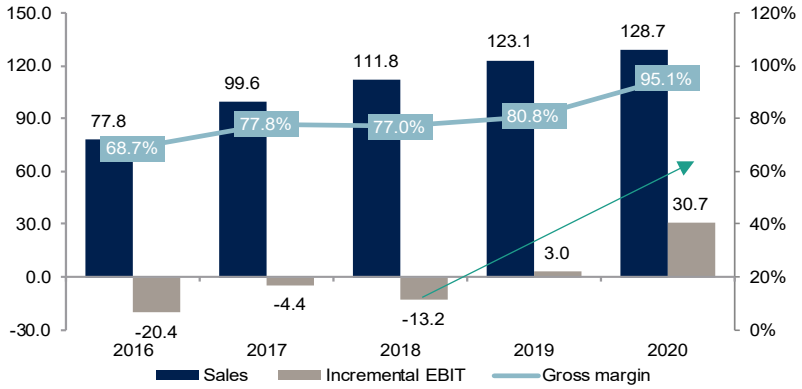
Source: ABG Sundal Collier, company data

Cost items moving in the right direction



Source: ABG Sundal Collier, company data

Solid development in incremental EBIT following the strategic shift



Source: ABG Sundal Collier, company data

Roadmap to profitability

After realigning its strategy, the roadmap to profitability is now the focus for the company. We believe that Clavister has what it takes to become profitable – it has the right customer relationships and the right product portfolio. Now it needs to execute on that. With a relatively fixed cost base, growth is the main factor to drive profit. Its ambition is to achieve a CAGR of 20% and be free cash flow positive in 2022. Due to positive developments in recent years, we believe its ambitions are attainable. If the company manages to achieve a CAGR of 20% for a longer period, then we believe that the long-term ambition of profitability levels in line with its peers is attainable as well.

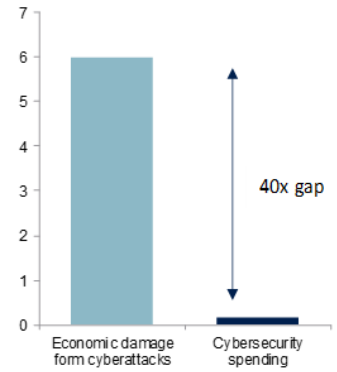
Clavister's financial ambitions

2021	Mid-term (next three years)	Long-term
• Outgrowing the underlying market • Grow sales y-o-y • Reach sustainable EBITDA margin	• Outgrowing the underlying market • Net sales CAGR of +20% • Positive FCF from 2022	• Provide industry leading profitability and FCF (implies profitability in the 25-30% range)

Source: ABG Sundal Collier, company data

The opportunity

Damages are 40x the spending, (USDtn)



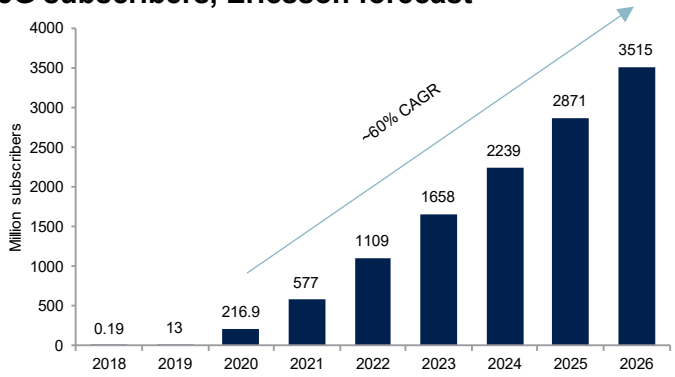
Source: Cybersecurity Ventures, Gartner

Several market trends drive the demand for cybersecurity, such as digitalisation, 5G and geopolitical tensions. Ultimately, we believe the main driver is the damages associated with cybercrimes. It is expected that damages from cybercrimes will amount to USD 6trn in 2021. This is 40x the amount currently spent on cybersecurity each year. We think increased awareness, but also regulation and frameworks put forward by governments and institutions will accelerate the spending on cybersecurity.

5G ramp-up

We currently see the 5G ramp-up as the most significant growth driver. Ericsson forecasts that 5G adoption in Western Europe will increase from 1% in 2020 to 69% in 2026. Clavister has already licensed its 5G security solution to ~5% of all mobile operators and generates revenue based on traffic volumes on their networks. We estimate an addressable market for Clavister from mobile operators of ~SEK 400m to ~SEK 1200m. We estimate that Clavister had approximately SEK 30m in 5G revenue in 2020, a number that we think could double in the next two years.

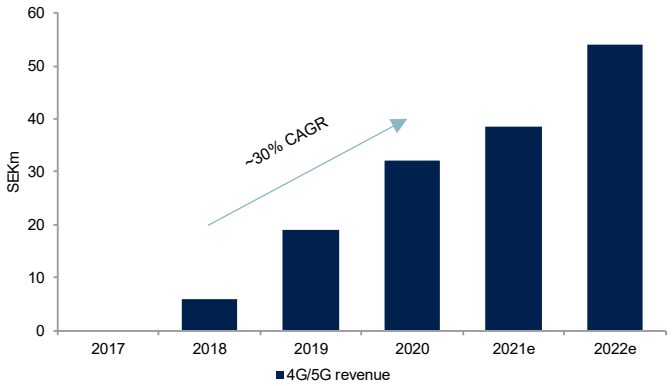
5G subscribers, Ericsson forecast



Source: Ericsson mobility report 2021

Clavister 4G/5G revenue, ABGSCe

Reported numbers for 2018 and 2019, ABGSCe for 2020



Source: ABG Sundal Collier, company data

Future-proofed enterprise offering

According to Gartner, SASE is the future of cloud security for enterprises. Clavister has developed its own SASE solution, which is expected to be launched in H2'21. Importantly, Clavister's offering is based on +75% proprietary software, which is a significant strength compared to competitors. As far as we know, there are no other European vendors that are expected to launch SASE solutions.

Opportunities in the defence industry

Clavister secured its first defence contract last year, worth SEK 50-90m. Together with BAE Systems, Clavister is developing cybersecurity for armed vehicles for a western military force. We expect more orders like these to come, as cybersecurity will be mandatory for all new vehicles from 2025, either through BAE Systems, or other OEMs.

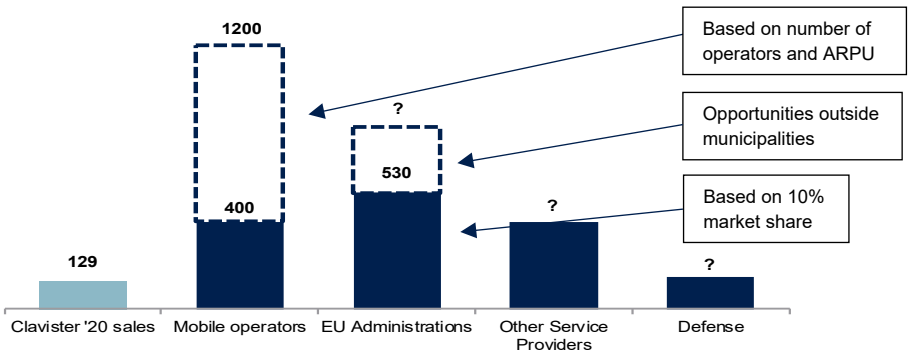
Geopolitical tensions and regulation benefits local security vendors

Our assessment is that geopolitical tension and data privacy regulations benefit firms like Clavister. In addition, as a European vendor, Clavister has a competitive advantage versus US- and Israel-based competitors, in our opinion. (See more in the *Growth opportunities* chapter).

Directly addressable market worth SEK 900m-1,700m

Looking at potential public administration customers in Sweden and Germany, as well as 5G security for mobile operators, we arrive at a directly addressable market worth SEK 900m-1,700m for Clavister. These numbers imply 30% market share in public administrations and partnerships with 5% of mobile operators.

ABGSC estimate of Clavister's directly addressable market, (SEKm)

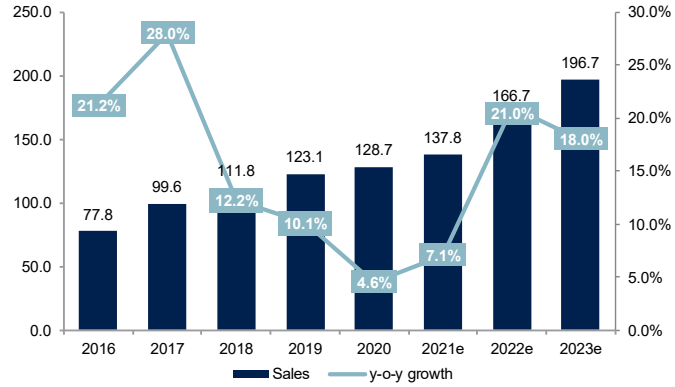


Source: ABG Sundal Collier estimates, company data

Forecast

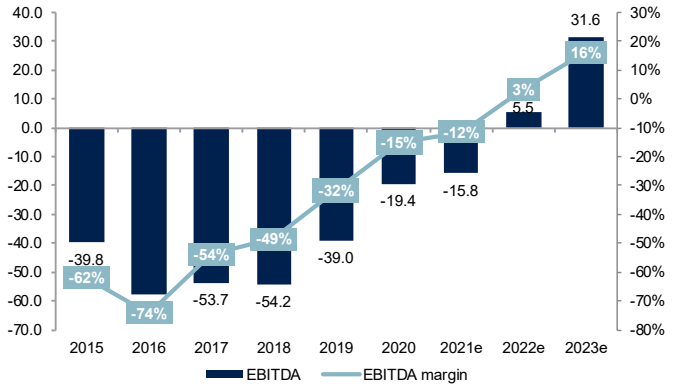
Clavister's ambition is to grow by 20% p.a. and increase its market share. In the near-term ('21e-'23e), we forecast a 19% organic sales CAGR, mainly driven by the 5G roll-out and delivery of the BAE Systems contract. Moreover, we expect that opex will remain relatively flat over the same period, allowing Clavister to scale on its cost base. This should result in positive EBITDA in 2022 and EBIT in 2023. In terms of EBITDA, we pencil in '22e-'23e margins of 3% and 16% respectively.

Sales and sales growth y-o-y (SEKm)



Source: ABG Sundal Collier, company data

EBITDA and EBITDA margin (SEKm)



Source: ABG Sundal Collier, company data

Valuation – fair value range of SEK 5-16 per share

To arrive at a fair value range for Clavister, we have looked at peer multiples of international cybersecurity firms, and constructed a DCF model with three scenarios. In the peer valuation, we looked at EV/sales and EV/EBITDA multiples, and compared them to sales growth. In the DCF, we use three different spans of growth rates (13% to 20% CAGR) and profitability levels (14% to 17% avg. '25e-'30e EBIT margin). By using a blend of the two methods, we arrive at a fair value range of SEK 5-16 per share. This implies a '22e EV/sales of 3x-7x. We estimate that Clavister will grow its sales by a 19% CAGR from '21e to '23e, and reach positive EBITDA in 2022e.

Business model

Clavister primarily targets three customer segments: service providers, public administration, and defence contractors. It has designed six specific solutions, tailored to their specific needs. The revenue model is mostly recurring revenue, while a small part comprises hardware and consulting fees.

Six solutions to address specific industry challenges

Clavister has developed six solutions for its customers. Over time, the solutions are being complemented with additional functionality. The solution set consists of SASE (a cloud-native SD-WAN+ solution), the Next-Generation Firewall, Secure SD-WAN, Identity & Access Management, 5G security as well as Cyber Armour. Some of the solutions are overlapping. Next-Generation Firewall and Identity and Access Management, for instance, are both important components of the SASE solution, but are also offered on a standalone basis.

Clavister solution set

Source: ABG Sundal Collier, company data

Recurring revenue model

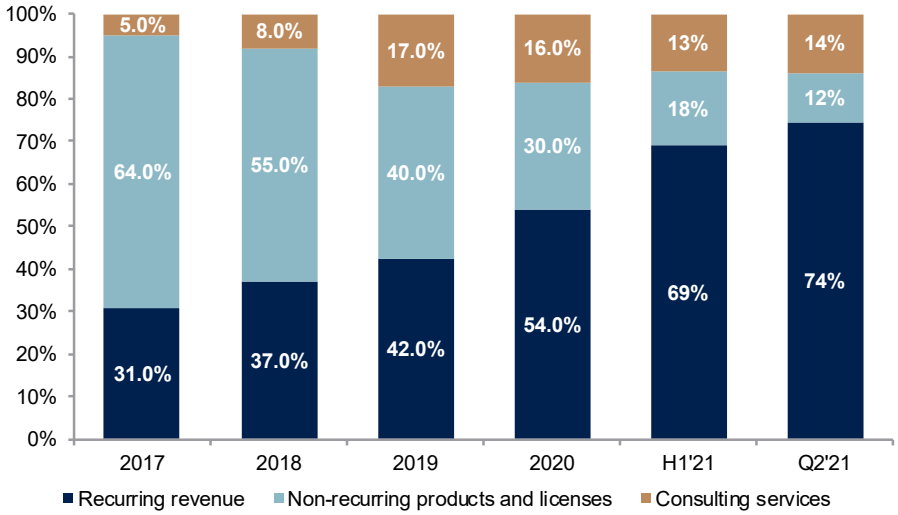
With its new strategy, where it is transitioning from a product seller to a solution provider, Clavister is also consolidating its revenue model to a recurring revenue model to help facilitate this change. Earlier, it had different revenue models that varied depending on multiple factors. Today, the revenue model is being consolidated to a uniform multi-tier as-a-service model, including a base offering that allows for a simple and less expensive onboarding. For some solutions, like the 5G and Defence solutions, the revenue model is a bit different; for the 5G solution, for example, some customers are charged based on maximum data capacity. For the Defence segment, the revenue is mostly project-based.

Consolidating the revenue model

Source: ABG Sundal Collier, company data

The company has been successful in transitioning to a recurring revenue model. Last quarter (Q2'21) recurring revenue constituted 74% of total revenue. We think that the phase-out of non-recurring and hardware revenue could have had a negative impact on growth during the transition. In the second half of 2021, the company is rolling out its SaaS model. The aim of this model is to further reduce the hurdle for new clients to on-board, while possibly also facilitating higher customer retention due to the structure of the SaaS model.

Transitioning to a recurring revenue model



Source: ABG Sundal Collier, company data

Customer segments and targeted solutions

Most customers only use one of the six solutions Clavister offers, which we see as indicating that there is a lot of potential for up-selling. In addition, the company's new pricing strategy, based on a multi-tier model, allows for customers to upgrade to a more advanced solution, which generates more revenue for Clavister. Several important trends drive demand for Clavister's solutions. The picture below highlights some of them, as well as market sizes, growth and key customers.

Market overview of the three main customer segments and solutions catering to their needs

Industry	Key market trends	Solutions	Customers	Market
Service Providers	• Increasing complexity drives trend of out-sourcing security to service providers • The adoption of 5G drives cybersecurity investments to ensure network resilience • 5G capabilities opens up for over-the-top security services to enterprises	• Identity and access management • Next-Generation Firewall • Secure SD-WAN • Clavister SASE • 5G Security	• Telco • Tata Com. • Nokia • Ericsson	• USD 34bn • CAGR 8%
EU Public Administration	• Digitalisation of government services • Implementation of cybersecurity regulations • Large financial impacts of cyberattacks on critical infrastructure and government data • Increasing public-private partnerships	• Identity and access management • Next-Generation Firewall • Secure SD-WAN • Clavister SASE	• MSB • CSN • Försäkringskassan • Göteborgs stad	• USD 15bn • CAGR 8%
Defence	• Modernisation and cloud migration • Digitalisation of military operations • Successful cyberattacks may lead to loss of mobility and critical communications, or interception of intelligence	• Cyber Armor • Identity and Access Management • Secure SD-WAN	• SAAB • BAE systems • Digital Cloak	• USD 10bn • CAGR 8%

Source: ABG Sundal Collier, company data

Service Providers

Among other services, Service Providers offers its customers a wide range of solutions, including cybersecurity licensed from cybersecurity vendors. Moreover, it usually handles the deployment of technology and offers 24/7 monitoring, security, and firmware updates. Having a service provider may relieve the burden of day-to-day operations and management of connectivity and security products. Service providers that are partners to Clavister usually belong to either Communication Service Providers or Managed Security Service Providers (MSSPs). CSPs provide 5G and other network services, primarily to mobile operators, while MSSPs provide WAN solutions and other network solutions for enterprises. In recent years, Clavister has secured partnerships with global service providers like Tata Communications and Telco Systems on the enterprise side, and Nokia on the mobile operator side. Many of these partnerships are just entering commercialisation. That said, we expect these partners to roll out new systems, with embedded security provided by Clavister in coming years. Also, we anticipate the company to continue attracting more mobile operators to its 5G security solution.

EU Public Administrations

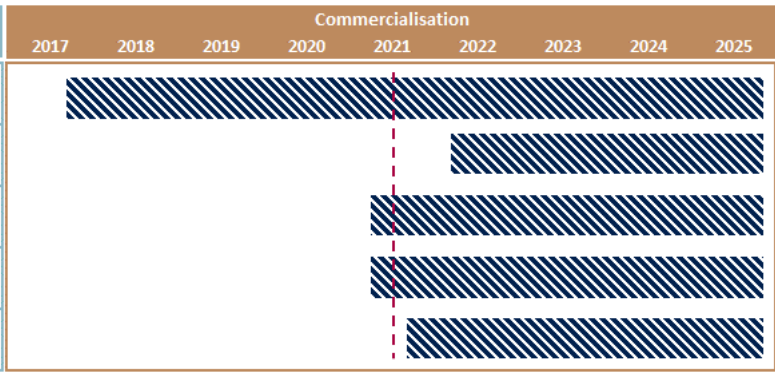
These mainly consist of public administrations in the Nordic region. According to Clavister, many of the critical Swedish agencies have chosen Clavister as a security provider. Clavister typically reaches public administrations through system integrators, like Tieto or ATEA. As a European cybersecurity leader, we expect that Clavister will gain a similar position in other EU countries. With intensifying geo-political tension as well as regulations like the EU Cybersecurity Act – implemented to secure Europe's competitiveness in the cyber space – we think that Clavister is well positioned to benefit.

Defence

This customer segment consists of OEMs and defence subcontractors that want to or are required to incorporate cybersecurity functionality into military vehicles, equipment or enterprise networks (used by defence agencies). Clavister has recently partnered with BAE System's Swedish subsidiary Hägglunds, a manufacturer of military vehicles. Clavister and BAE received their first defence contract in 2020, worth SEK 50m with SEK 90m potential. We expect more contracts to come from this platform, and potentially new platforms as well.

Overview of some of Clavister's recently announced major partnerships

Announced	Partner	Details
2016	Nokia	Virtual security for telcos and mobile network operators
2018	Tata Communications	Alliance to deliver packaged solutions for CSPs around the world
2019	Telco Systems	Virtual security to industrial IoT, automotive and other customers
2020	Digital Cloak	Deliver IAM solutions to the US DoD. Currently pilot w. the Marine Corps
2020	BAE Systems	Military vehicle with embedded security from Clavister



Source: ABG Sundal Collier, company data

The sales organisation is an integral part of the strategic shift
The aim of the strategic shift is to take advantage of the company's inherent scalability, specifically the high gross margin, to drive profitability. The company's sales organisation is an important part of its strategy.

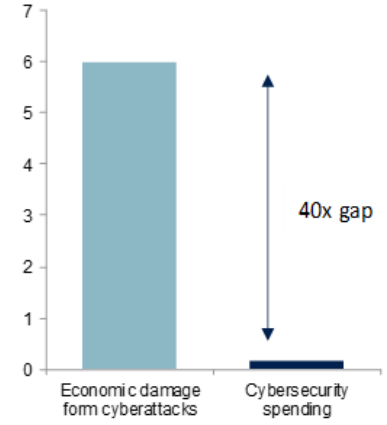
A sales organisation designed for scale
The sales organisation can be divided into three parts: channel management, business development managers (BDM) and key account managers (KAM). Channel partners are important for Clavister's business model. Although Clavister usually talks directly to the end-customer, channel partners are important for delivery and installation. Moreover, public administrations usually purchase via frame agreements with selected distributors. As such, it is difficult for Clavister to sell directly to the administration. Channel partners are also important, as Clavister can reach many potential customers through them, which offers significant scale opportunities. Important partners include Atea, Tieto and Certezza.

BDMs primarily work in the Nordics and Germany, and their purpose is to create new business opportunities with larger accounts such as public administrations. Once a business opportunity has been put into place, channel partners are then brought in. KAMs work with established large accounts like Nokia, BAE Systems and IWG. Nokia can also be seen as channel partner, as Clavister reaches mobile operators through Nokia. Similarly, BAE Systems is a channel for Clavister to reach Defence customers.

Addressable market

Clavister's total addressable market in 2021 is forecasted at ~USD 60bn, with an estimated '21e-'23e CAGR of ~8%. With total cybersecurity spending 40 times less than total cyberattack damages, we believe that spending will continue to grow at this rate for a long time. We estimate that Clavister's directly addressable market for the two public administration segments in Germany and Sweden, plus 5G security for mobile operators, is worth between SEK 900m-1,700m. Our assumptions are based on Clavister directly addressing 10% of municipalities in Sweden and Germany and 30% of mobile operators (through partnerships with Ericsson and Nokia). Clavister currently has partnerships with ~5% of the mobile operators. These assumptions do not consider any sales from defence contracts or SD-WAN/SASE solutions.

Damages are 40x the spending, (USDtn)



Source: Cybersecurity Ventures, Gartner

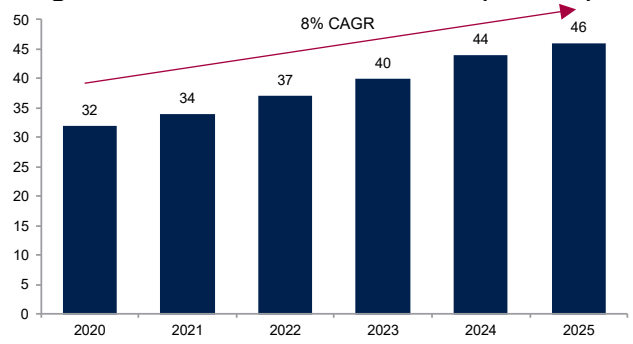
The total cybersecurity market

Considering that damages from cyberattacks are approaching USD 6trn, the incentives to pay for cybersecurity should be high. But Gartner only forecasts a worldwide security and risk management spend of USD 150bn in 2021 (+12% y-o-y growth)[1]. With spending representing less than 3% of damages, we expect spending to continue to grow at a steady pace to reduce the gap. Identity and Access Management, Cloud Security, and Security Services (including security outsourcing) – which constitutes Clavister's core offerings – will grow by 16%, 41%, and 11% respectively, on aggregate outperforming the cybersecurity market in 2021.[2]

Clavister's main markets

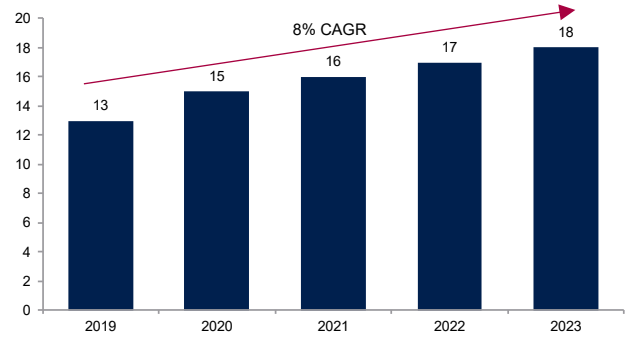
Clavister addresses three main market segments: the Managed Security Service market, EU Public Administration cybersecurity spending, and Global Defence cybersecurity spending. Together, these three are forecast to be worth ~USD 60bn in 2021, while growing at 8% annually from 2021 to 2023[3]. Other market research agencies forecast total market growth of 8-15% from 2021 to 2028[4].

Managed Service Providers market, (USDbn)



Source: Westland Advisory

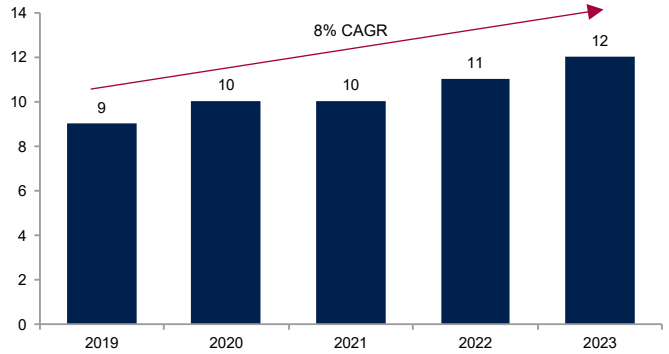
EU Public Administration market, (USDbn)



Source: Westlands Advisory

[1] Other estimates are: Quince, USD 180bn; Mordor Intelligence, USD 195bn; Grand view research, USD 180bn.
[2] According to Gartner.
[3] According to Gartner.
[4] According to Mordor Intelligence, Grand view research, Cybersecurity Ventures, and Quince.

Global defence cybersecurity spending (USDbn)



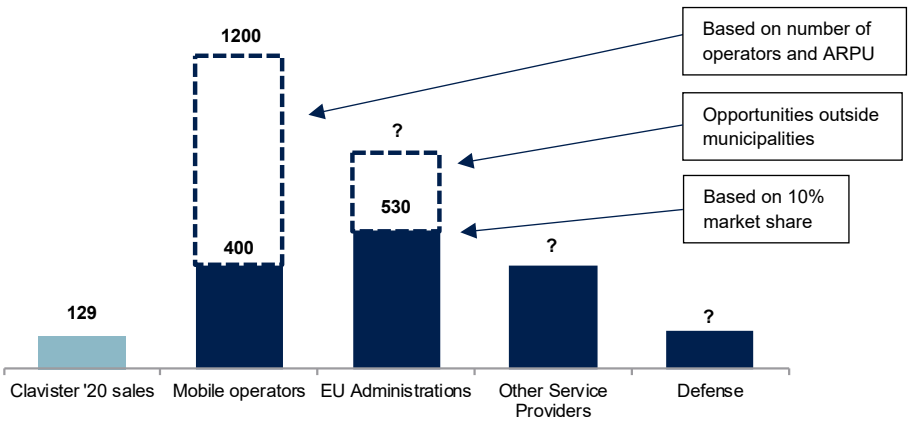
Source: Westland Advisory

But how much is achievable for Clavister?

We can estimate the number of mobile operators Clavister addresses directly through Nokia and Ericsson (today approximately ~30 out of 600-800 operators). We expect that this number can grow to 20-30% of all operators. Clavister has said earlier that average revenue per (small/medium sized) operator is SEK 3-6m annually.[5] Hence, we arrive at an addressable market of SEK 400m-1,200m, just for mobile operators. Right now, revenues from operators ought to be very low as the 5G adoption was below 5% in 2020.[6]

In terms of EU administrations, Clavister primarily targets Sweden and Germany. There are ~300 municipalities in Sweden and ~5,000 in Germany. If we assume SEK 1.0m[7] of annual revenue per municipality, the addressable market amounts to SEK 5,300m. A 10% market share would then imply SEK 530m in revenue – a market share we don't see as impossible (based on our impression from talking to management, we think the current revenue from this segment is SEK 30m-50m). We also emphasise that Clavister works with government agencies outside of municipalities, which provides additional upside to the estimate. Taken together (mobile operators and municipalities), we see a directly addressable market of SEK 900m-1,700m for Clavister. But this does not include any revenue from the defence business that we believe can bring in SEK 50m annually in a couple of years, nor SD-WAN and SASE revenue, which we find harder to estimate but expect will be important revenue drivers. In terms of total market size, Managed Security Services (i.e. SD-WAN and SASE) is the largest, with USD 30bn-40bn in annual spending. Spending on SASE solutions (a concept developed in 2019) alone is forecasted at more than USD 5bn in 2027, according to the company.

ABGSC estimate of Clavister's directly addressable market, (SEKm)



Source: ABG Sundal Collier estimates, company data

[5] Source: Clavister Business update 07/06/17.
[6] Ericsson mobility report 2021.
[7] ABGSC estimate based on received orders and the announced revenue from CSPs.

Value proposition

This chapter goes through Clavister's six security solutions, how they are integrated in systems provided by its partners, and how this creates value for the end-user. We find that Clavister has a strong value proposition for its three main customers – service providers, EU public administrations, and defence contractors. We expect that many customers value the fact that Clavister is an EU-based firm with backdoor-free products and no ties to governments with geo-political tensions. We also find that Clavister offers a very competitive virtualised security solution used in 5G networks, SASE solutions (the future of cloud security according to Gartner).

How Clavister creates value for its customers

"SD-WAN can bring down costs by up to 75%" – DELL

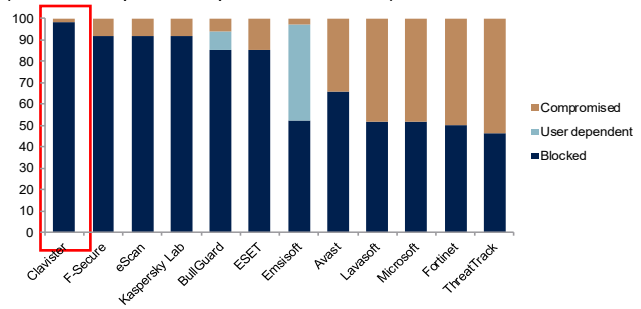
With a new product offering that is crisper and clearer, the company aims at capitalising on market trends that drives the need for more sophisticated and virtualised security solutions. Digitalisation, and later, the rapid emergence of remote working – not to mention the adoption of 5G that is expected to reach critical mass in the coming years – requires more flexible, agile, and scalable security solutions. Clavister stands firm with ready-to-ship security solutions that solves the security challenges enterprises and organisations face. Two factors stand out to us as Clavister's primary moats. The first being its strong portfolio of proprietary technology. We find that Clavister has a very competitive security offering for both mobile operators that want to secure their 5G networks and, Service Providers and system integrators that offer solutions for enterprises and governments.

Clavister Multi Factor Authentication solution is used by many critical government institutions in Sweden

Studies have shown that Clavister's products are performing at a world class level. A testament to that is that Clavister products are embedded in Nokia's flagship 5G security solution NetGuard. With Nokia, Clavister has deployed its virtualised solution **to 15 tier-1 operators** around the world. As Nokia's customers start ramping up 5G subscriptions, Clavister will benefit from higher licensing fees that scales with users and data volumes. In addition, Clavister is the security provider to Telco Systems new enterprise solution that targets SMEs. New enterprise networking solutions like SD-WAN and SASE are estimated by Gartner to reduce network costs by up to 75% – with adoption still below 50%. Moreover, as more enterprises migrate their networks to the cloud, we expect that Clavister will benefit in terms of upselling as more sophisticated functionalities are added to the offerings.

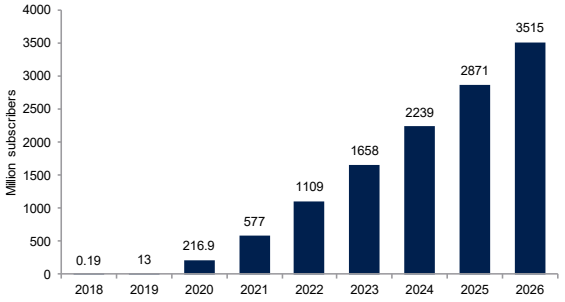
Another testament to the technology's performance is the partnership with BAE Systems signed in 2020, proving that Clavister's solutions are fit for military use. The second major moat is being an EU-based vendor. This gives Clavister an advantage in signing EU public administrations and military OEMs as customers, as well as firms that seeking compliance with EU regulation. Lastly, as a Swedish vendor, Clavister's solutions are backdoor-free – a major competitive advantage, as many of its international peers have been vulnerable to backdoor bugs.

Survey: Performance of Endpoint Security
(Clavister in partnership with Bitdefender)



Source: AV-Comparatives, Heuristic/Behavior Test

Number of 5G subscriptions worldwide, forecast

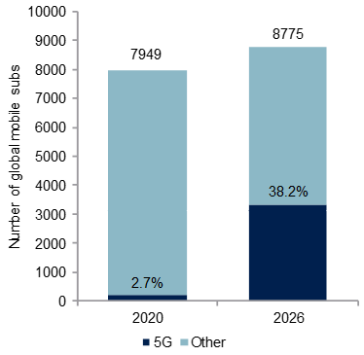


Source: Ericsson mobility report 2021

5G – The journey has just started

In many ways, 5G networks are much more vulnerable to cyberattacks compared to 4G. First, one of the core enablers of 5G is the higher frequency of smaller cell towers that connect the network. In addition, in 5G networks, core network functionalities have been virtualised and moved from the core network to the edges of the network. With the virtualisation, third party providers are invited to tap into the network and provide functionalities. With more parties involved, virtualisation of core functionalities and more entry points, new security challenges have emerged. Clavister is a leading provider of scalable, virtualised network security, offering tailored solutions for 4G/5G Service Providers. With Clavister's solutions, networks are secured from the edge via the core and all the way to the internet or other networks. Its 5G solution has been developed for telecom, and its robustness and integration capabilities fine-tuned in collaboration with tier-1 operators.

5G adoption (mobile subs)



Source: Ericsson mobile report 2021

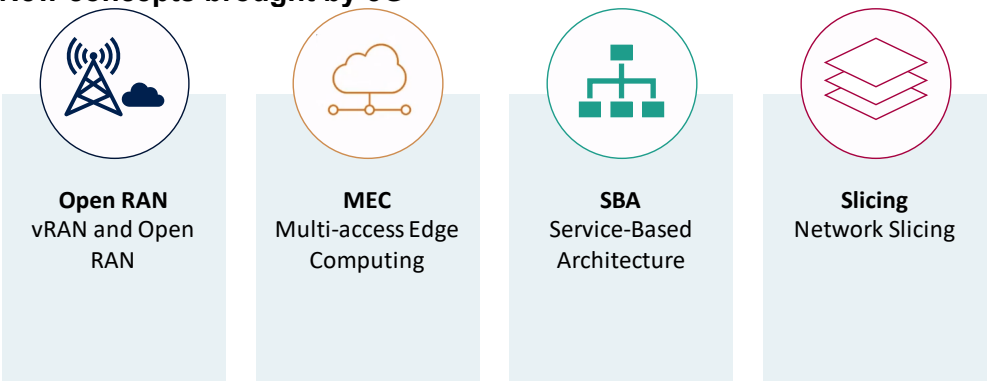
The journey from 4G to 5G – slow but steady

The transition is far from an overnight switch, and the two will likely co-exist for a long time. The journey has started with the addition of 5G base stations to the 4G networks, adding features including higher frequency. Going forward, operators will start migrating subscribers to 5G gradually. According to a study from Heavy Reading, 56% of respondents (operators) say they plan to start deploying 5G before the end of 2021 while 44% plan to have started in 2023 or later. But 'start deploying' does not mean that all mobile subscribers will be migrated instantly, nor that the network core will be 5G based. According to Ericsson, 5G subscriptions only constituted 3% of total subscriptions in 2020. Ericsson forecasts that adoption will reach 38% by the end of 2026. The migration is expected to advance more rapidly in North America and Western Europe where Ericsson forecasts 2026 adoption of 84% and 69% respectively. This is important as Clavister generates revenue based on number of users and traffic volumes. Hence, we expect that the current level of 5G revenue is low but will start to have an impact on group level revenue in the coming years.

5G brings new concepts

In a nutshell, 5G is like other networks, but it adds a couple of new concepts that brings more complexity, which creates new security challenges. Radio networks (RAN) have traditionally been proprietary technology provided by large network providers like Ericsson, Nokia, Huawei, etc. These technologies can now be deployed using **Open RAN**, which provides an open environment where APIs allows more vendors to provide different functions in the network. This adds to the complexity of the network as security will be affected by more vendors providing critical infrastructure with potential access to sensitive data. Then there is the concept of **Multi-Access Edge Computing** (MEC). 5G is built on the promise of low latency. Low latency is required for important 5G use-cases like self-driving cars, where low latency is mission critical as cars need to communicate in real time. MEC supports the low latency requirements by moving the datacentre – where critical data must flow through – out to many mini-datacentres at the edges of the network, closer to the device. One of the main improvements of the 5G network is its **Service-Based Architecture** (virtualisation), which enables cloud-based core network functionality. The virtualisation allows operators to manage network capabilities on demand using software-based applications where hardware boxes once stood in the architecture. Finally, there is **Network Slicing**. An innovation that provides the ability to "slice" the network into different "virtual networks", designed to meet different requirements.

New concepts brought by 5G



Source: ABG Sundal Collier, company data

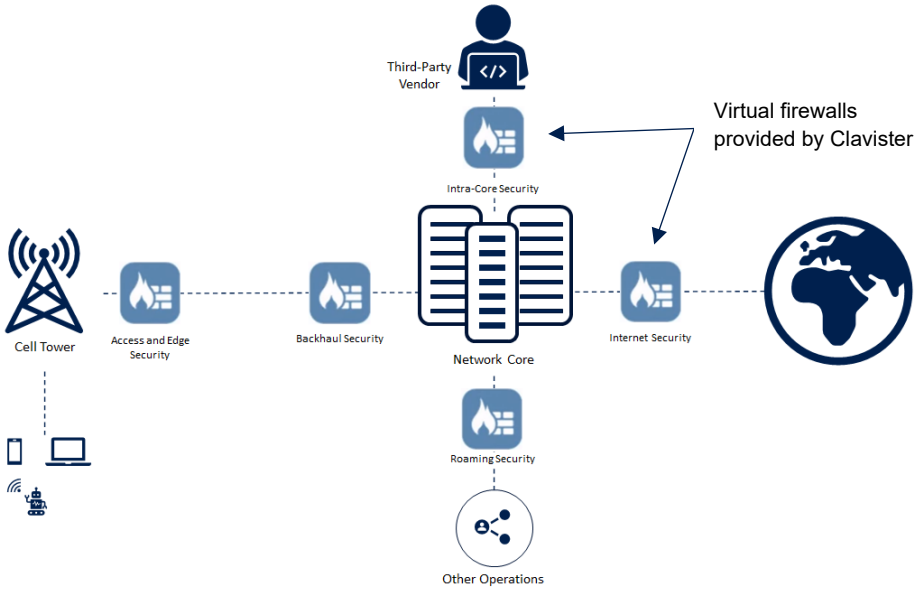
Threats

Most threats to 5G networks come from one of three sources: 1) The edges where there is risk of intrusion, and malware entering the network and spreading to the core. 2) From within the core network. As this is a place where sensitive data is stored, managers accessing the network remotely might carry malware that compromises important data or functionalities. 3) The Internet is where a significant part of the traffic is headed. Threats from the Internet mainly consist of DDoS attacks and application vulnerabilities. Another common threat are fake base stations. Fake stations have been deployed outside of the Whitehouse for example, as well as outside of the Swedish Parliament. Mobile devices may connect to the fake stations allowing the attackers to intercept data traffic.

Securing the 5G network

With more control functionality moving to the edges of the networks, security must follow. 4G security is all about securing a very centralised, static, and predictable core[8]. Hence, 5G security is very different. Protection in a 5G network is required from the edge to the core and out to the internet, similar to a SASE environment. Clavister Service-Based Firewall, a virtual firewall solution, can be deployed at all edges of 4G/5G networks, as well as in the core. With zero-touch deployment, networks can scale up efficiently by bringing on new security points in seconds.

5G Security, protection from the edge to the core



Source: ABG Sundal Collier, company data

[8] According to Fortinet.

Clavister 5G security – use cases

Clavister 5G Security offers operators a smooth migration from 4G to 5G as the technology is compatible with both systems. Moreover, the solution is built on fully virtualised firewalls, made in Sweden by Clavister, guaranteed as backdoor-free. Finally, Clavister NetShield Virtual, was formally validated by Intel as the fastest virtualised solution for securing 5G networks, in May 2021.[9]

Backhauling

Backhauling is the link between a remote site – where equipment like cell towers are located – and the Core Network (i.e. the management node). With 5G comes increased density of base stations. In addition, in phase 2 of the 5G deployment (Release 16) wireless backhauling has been standardised for situations where fiber is not feasible or too costly to deploy. As a result, backhauling is becoming an even more critical part of the network. Clavister secures the 4G/5G backhaul and ensures reliability and privacy by encrypting all traffic that flows through untrusted networks.

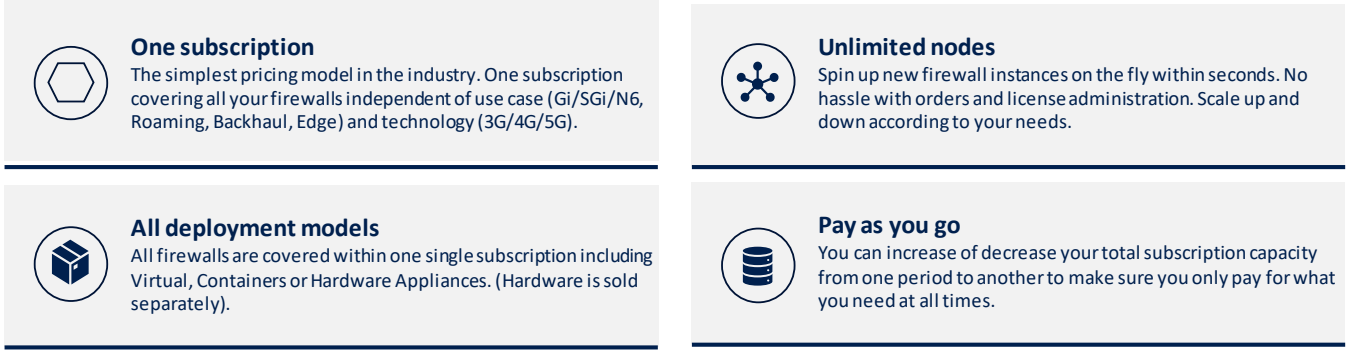
Internet security - Firewall

According to Clavister, analysts predict that the number of connected devices will double within a few years. Not only would the number of devices increase, so would the amount of data traffic, especially with the introduction of 5G. With the rapid growth in data traffic, firewall solutions must be able to scale without adding more costs for the customer. According to Clavister, its firewall solutions (NetWall and NetShield) offer the highest security performance on the market, for both hardware appliances and virtual solutions. It offers solid DoS protection with Traffic Anomaly Filtering. Clavister Firewall solutions are used by customers throughout their networks, from the edge to the core.

Edge security

The solution to solve the low latency requirements that 5G networks offer, is to move central network functions to the edge, close to the base stations. As a truly distributed cloud network, 5G means that security functions can no longer be enforced only at a traditional perimeter entrance point. Instead, security is a prominent concern in every corner of the network. Critical security functions such as Firewalling, Antivirus Scanning and Network Attack Protection need to follow and be deployed at the edges of the network. Clavister's Service-Based Firewall (SBFW) solution and Intrusion detection and prevention system provides Edge Security for 5G networks. Service-based firewalling is taking an established security function and deploying it as a virtual solution at the edges of a network, while adding new functionalities.

Cloud native pricing model



Source: ABG Sundal Collier, company data

[9] https://www.clavister.com/clavisters-5g-security-performance-validated-with-intel/

5G adoption

According to Ericsson, 5G subscriptions only constituted 3% of total subscriptions in 2020. Ericsson forecasts a gradual adoption that reaches 38% globally by the end of 2026. The number of 5G subscriptions is expected to reach 3.5bn in 2026 vs. 211m in 2020. Adoption in Clavister's core market, Western Europe, is expected to increase from ~1% in 2020 to 62% in 2026. This is important as Clavister generates revenue based on the number of users and traffic volumes. Hence, we expect that its current level of 5G revenue is low but will start to have an impact on group level revenue in the coming years. In addition, as Clavister has already developed its solution and already has licensing agreements in place with leading Service Providers like Nokia and Ericsson, we expect that it will see significant scale effects as operators bring users onto the 5G networks. Through Ericsson and Nokia, Clavister's 5G security solution is licensed to ~30 mobile operators, or ~5% of the market.

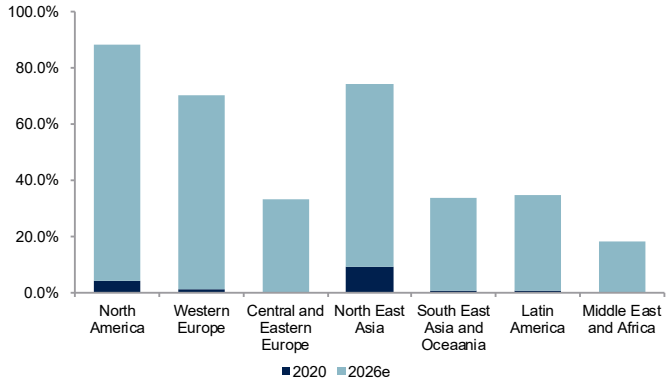
Adoption around the world

In Western Europe 4G is still dominant, with 78% of all subscriptions. 5G penetration in 2020 was low, at only ~1%. But, more than 60 Service Providers have already launched 5G services across the region, and Ericsson expects that 5G penetration will reach 69% by the end of 2026.

In North America, commercialisation of 5G is moving at a rapid pace. Here, Service Providers have launched commercial 5G services. By 2026, Ericsson forecasts more than 360m 5G subscriptions, accounting for 84% of mobile subscriptions.

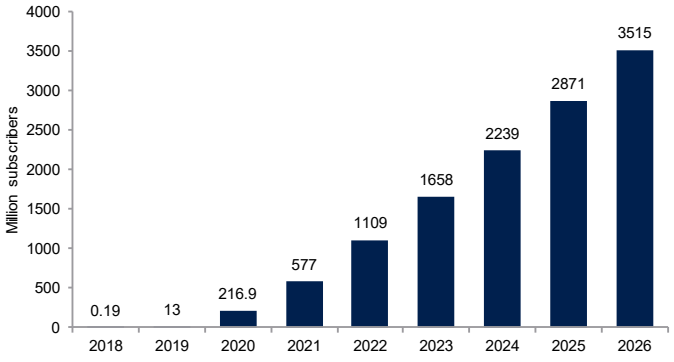
In North East Asia, Service Providers continue to invest to fuel 5G subscription growth. In 2020, the region showed an impressive 9% penetration. The current focus of Service providers is to improve nationwide coverage. Ericsson forecasts 1.4bn 5G subscriptions by the end of 2026, corresponding to a penetration of 65%.

5G adoption by region (2020 vs. 2026)



Source: Ericsson mobility report 2021

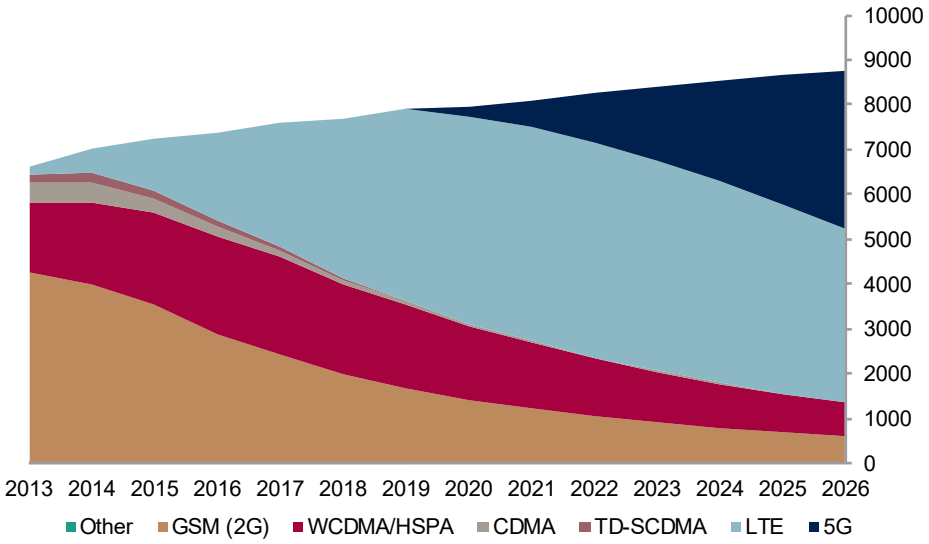
Global 5G subscribers, forecast



Source: Ericsson mobility report 2021

According to Ericsson, the migration to 5G will become the fastest migration to a new network technology in history.

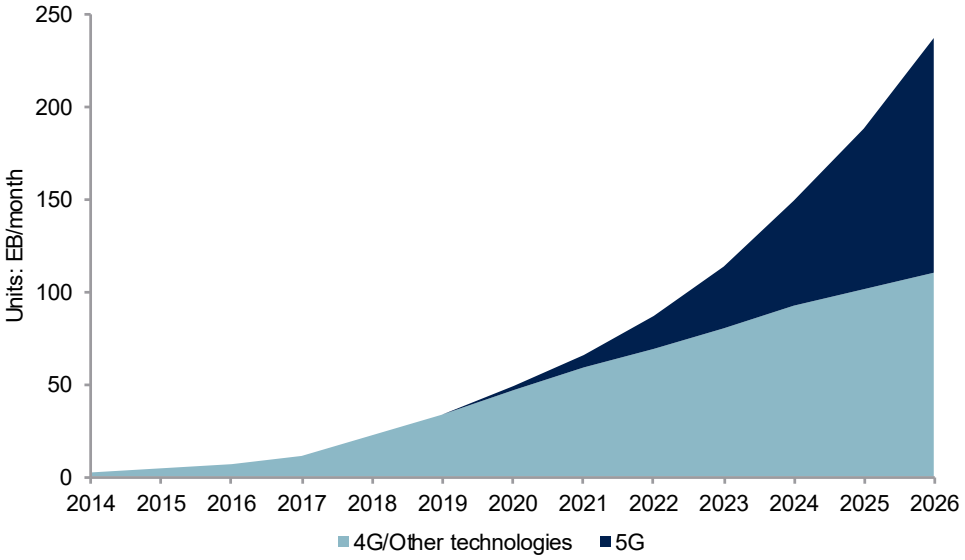
Mobile subscriptions by technology, in millions



Source: Ericsson mobility report 2021

Data traffic has been growing rapidly and will continue in a similar fashion. In just a couple of years, 5G will dominate data traffic volumes with more than half of total data volume.

Global mobile data traffic, by technology



Source: Ericsson mobility report 2021

Communication Service Providers references[10]

Nokia licenses Clavister Virtual Firewall and sells it under Nokia NetGuard
Clavister and Nokia entered a strategic partnership in 2016 to develop and deliver advanced virtual security solutions for mobile operators. Nokia is one of the world's top three infrastructure vendors, serving most of the largest global operators. Nokia has integrated Clavister's Service-Based Firewall solution, NetShield, into the Nokia NetGuard offering that protects network infrastructure and subscriber data from cyberattacks. For each telco operator that licenses Nokia NetGuard to secure their network, Clavister will book a recurring license fee without further effort. According to Clavister, its NetShield solution constitutes a significant part of the Nokia NetGuard offering.

"Powerful firewall with massive performance, ideal for virtualised telecom networks"
With Nokia, Clavister has deployed its virtualised solution **to 15 tier-1 operators** around the world.

Nokia and Three UK to deploy world's first next-generation cloud native core network
"Deployment will include the Nokia AirFrame data center, IP routing and network management, Nokia CloudBand™ Nuage Networks software defined networking, evolved packed core, IMS, TAS, SBC, Shared Data Layer and security solutions"

Vodafone India deploys Nokia Cloud Packet Core
"Various components of Nokia's Cloud Packet Core solution, including Nokia Cloud Mobile Gateway, CloudBand, Smart Plan Suite, NetGuard Security, DNS, and Cloud Signalling Director, are being used in this deployment"

NTTBP Appoints Clavister to Secure its Public Wi-Fi Service Network in Japan
"NTT-BP has selected Clavister and its integrator partner MIRAIT to implement security on NTTBP's extensive public Wi-Fi network, which has over 220,000 access points across Japan. The security deployment will also support NTTBP's network plans ahead of the 2020 Olympics in Tokyo"

[10] Source: Clavister.

Secure SD-WAN (Software Defined Wide Area Network)

"SD-WAN is the fastest technology adoption that we have ever seen" – IDC

Software-Defined Wide-Area-Networks (SD-WAN) is basically a software overlay on top of traditional on-prem WANs (traditional networks use Multiprotocol Label Switching [MPLS], Digital Subscriber Line [DSL], etc. for connection). SD-WAN facilitates the use of a less expensive broadband connection. In addition, it can connect all branches of the network to a centralised control network in the cloud, which brings increased speed, agility, and flexibility to the data routing. It is offered by Service Providers as a way for organisations to outsource their network management. With the growing complexity of networks, outsourcing network management is becoming increasingly popular. SD-WAN is also the perfect network solution for organisations that want to transition to a cloud-based infrastructure but are not ready to completely abandon the private infrastructure with higher security.

Service Providers licenses Clavister Secure SD-WAN to secure their networks

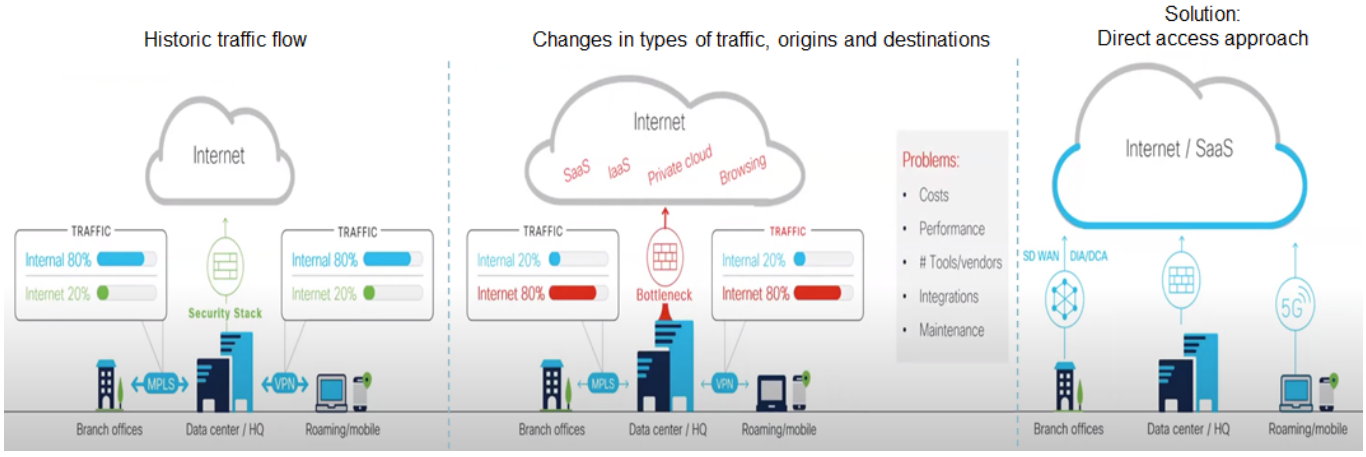
Most Service Providers, however, do not offer built-in security in SD-WAN solutions and are instead licensing third-party security solutions. Clavister has partnered with several Service Providers, including Tata Communications and Telco Systems, that incorporate Clavister's Secure SD-WAN solution in their offerings. Clavister's Secure SD-WAN solution includes on-premise and virtual firewall solutions and anti-virus, as well as its cloud-based management and analytics platform Clavister InCenter.

The old way of networking is slow and expensive

"SD-WAN can bring down costs by up to 75%" – DELL

Remote working and SaaS apps are the new normal, making the old way of networking slow and expensive. Traditional WAN infrastructures are run with a centralised private data centre where all traffic flows through. As the sole entry point into the network, this is where most security functionality is situated. This means that branch offices or remote workers cannot interact with other offices or the Internet without going through the data centre. As data traffic has increased substantially with the emergence of cloud services etc., traditional WAN structures have become very expensive (for more info, see Appendix 1), while bottlenecks cause latency issues. With internet traffic growing exponentially, this structure is unsustainable, calling for more efficient ways to route data in a private network. In addition, traditional WAN reduces an organisation's ability to scale up as adding new branches to the network takes time and cost a lot of money.

Changes in traffic flows cause bottleneck issues in the traditional WAN structure

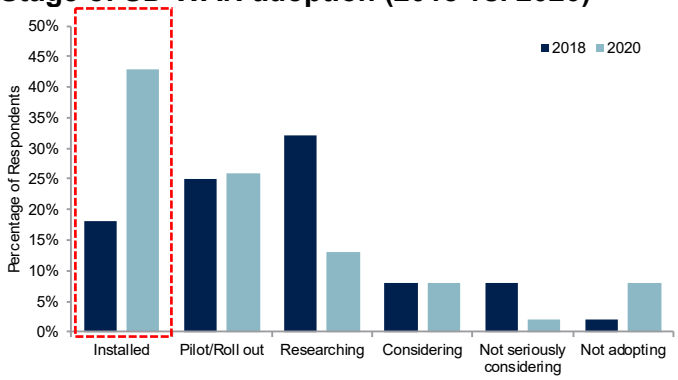


Source: ABG Sundal Collier, Cisco

SD-WAN enables organisations to cut their network costs by 75%

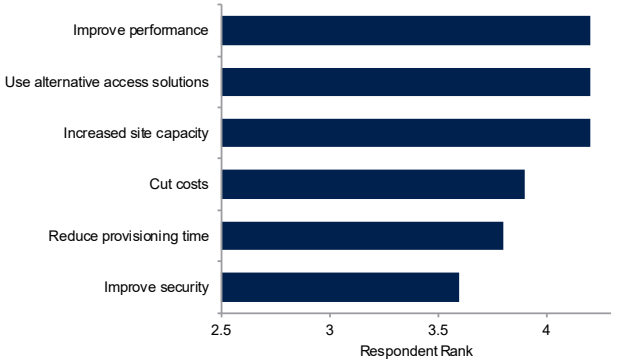
SD-WAN is the best way to get around the bottleneck problem that arises in traditional WAN[11]. The solution SD-WAN provides is a modern "direct Internet access approach". Going direct is much more efficient and reduces the need for a MPLS connection, which has been the standard way to connect network nodes. MPLS are very reliable, but also very expensive in terms of USD per bandwidth. Instead, less expensive transportation methods like 4G/5G or broadband can be used. According to Dell, substituting 50% of the MPLS lines for broadband can cut network costs by 50% or 75% by removing MPLS completely. In addition, SD-WAN enables zero-touch onboarding of new remote locations, which allows customers to scale up their organisations more efficiently. Based on the current adoption and its strong value proposition, we believe that SD-WAN is becoming the new network standard for enterprises not prepared to fully abandon the on-prem structure.

Stage of SD-WAN adoption (2018 vs. 2020)



Source: TeleGeography

Reasons for adopting SD-WAN (survey)

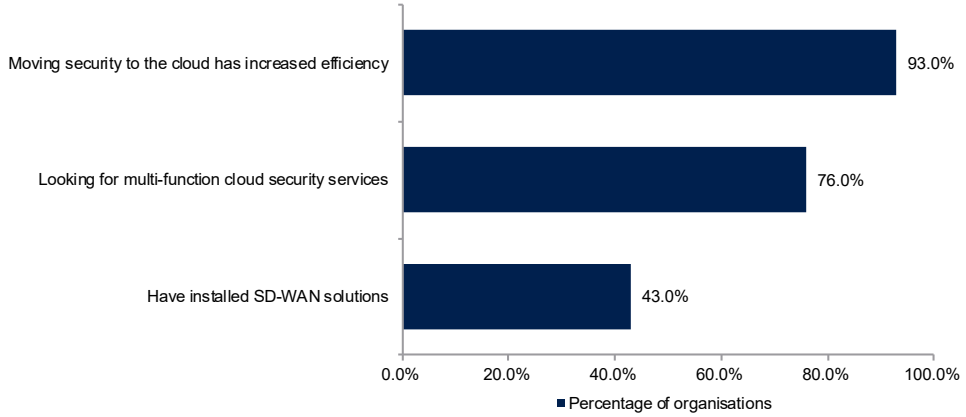


Source: TeleGeography

According to Cisco data, 93% of organisations have seen efficiency gains from adopting SD-WAN, 76% state that they are looking for cloud security services, but only 43% had installed SD-WAN infrastructure in 2020 (according to TeleGeography). The biggest challenge SD-WAN adoption faces seems to be that hackers realise that the network edges are more vulnerable to attacks compared to data centres (traditionally the only entry point into an enterprise network). This is important for SD-WAN vendors to take into consideration as organisations claim that branch offices are the source of compromise in ~70% of recent attacks[12]. Through its licensing agreement with Bitdefender, Clavister offers one of the best performing end-point security products on the market.

[11] According to Cisco.
[12] According to Cisco.

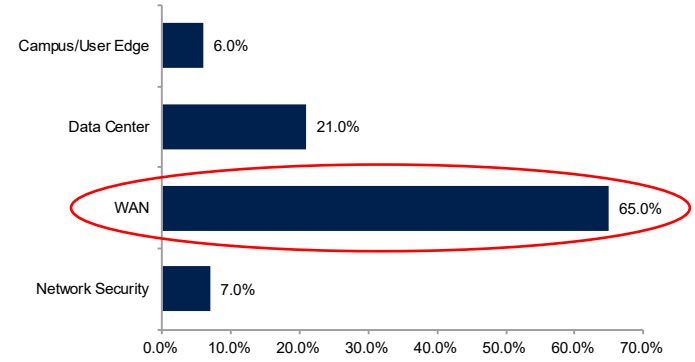
Organisations' agree on benefits from SD-WAN, but adoption still low



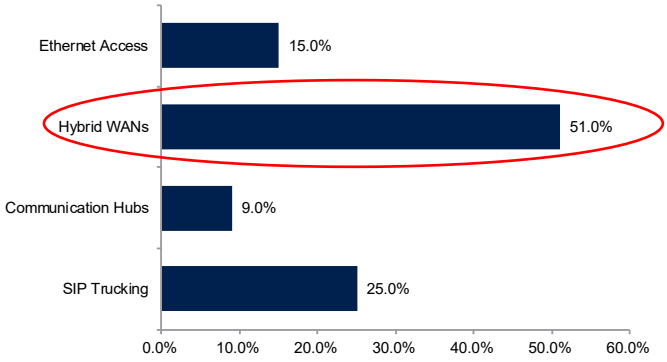
Source: ABG Sundal Collier, Cisco[13], TeleGeography

The driving force behind the adoption of SD-WAN in recent years has clearly been its cost competitiveness.

What portion of your network is most expensive? – Gartner Survey



What do you see as the biggest opportunity to cut network costs? – Gartner Survey



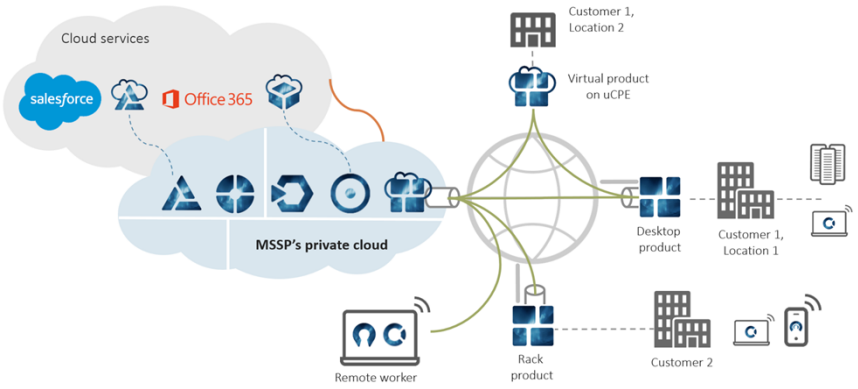
Source: Gartner Data Center Conference Dec 2015

New security challenges emerge from virtualising the network

But virtualising the network and removing the data centre as the only entry-point increases the vulnerability to cyberattacks. In SD-WAN structures, the security functions are therefore moved to the edges of the network, enabling users to access the Internet directly while still going through security. This is far more effective than aggregating security at the data centre, creating a choke point. Clavister Secure SD-WAN offers service providers protection from the network core to the edges and to the cloud. Security functionalities include hardware-based and virtual firewalls, VPN connections, and multi-factor authentication for access for all participants in the network (remote and on-prem). Clavister Elastic Cloud can be added to the offering, which forms a private portal for Service Providers to enable secure access cloud services (elastic because the solution grows depending on both traffic volume, user scale, and the number of use cases enabled, e.g. Virus scanning, Content Filtering, Traffic decryption, API layer scanning etc.). Moreover, the solution includes a central control centre for dynamic multi-path optimisation of the traffic, to ensure high security on sensitive data and to off-load the network, which reduces costs significantly. The Elastic Secure SD-WAN is a precursor to Clavister's upcoming SASE solution (expected to be launched in H2'21).

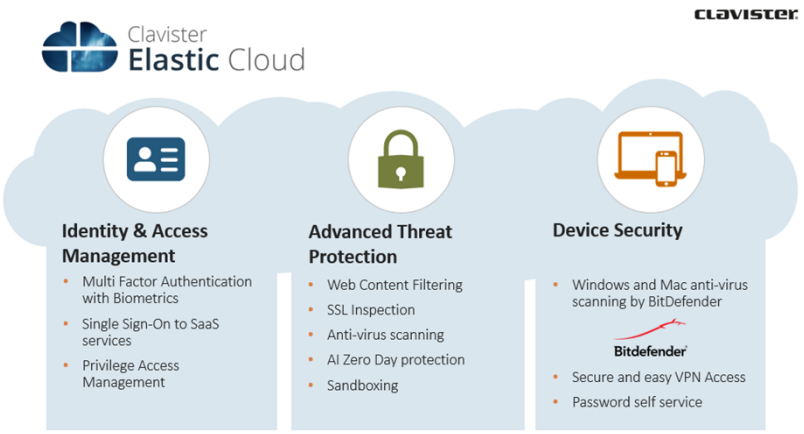
[13] https://www.youtube.com/watch?v=oa3xinNAOZo

How Service Providers run a secure SD-WAN with Clavister Secure SD-WAN



Source: company data

Clavister Elastic Cloud



Source: company data

Clavister is uniquely positioned as a European-based vendor

Clavister is the only European-based provider of completely virtualised security solutions that solves the security challenges Service Providers face with virtualised networks. Although competition is fierce in this space, new EU regulation to make the EU more digitally independent as well as escalating geo-political tension plays right into the hands of Clavister, likely making it a top candidate for Service Providers that want to be fully compliant with EU regulations.

What do the customers say about SD-WAN security?

Telco Systems

Telco recently announced its Fast SD-WAN offering ("Edgility"), a solution that challenges the paradigm of the traditional SD-WAN infrastructure.[14] It is an innovative solution that leverages multiple low-cost WAN connections per branch to ensure resilience and high quality access, and thus reduces the total service cost to a fraction of a similar SD-WAN offering. The solutions offer a cost effective and scalable solution for small businesses with an attractive ROI.

[14] Announced 7 July 2021: https://www.prnewswire.com/il/news-releases/telco-systems-to-challenge-the-sd-wan-paradigm-with-an-ultra-low-cost-plug-and-play-connectivity-and-security-suite-301326684.html

"We integrated a class A firewall and full security suite from our partner Clavister, and implemented powerful prioritized routing capabilities as well as smart failover on traffic degradation" – Ariel Efrati, CEO at Telco Systems

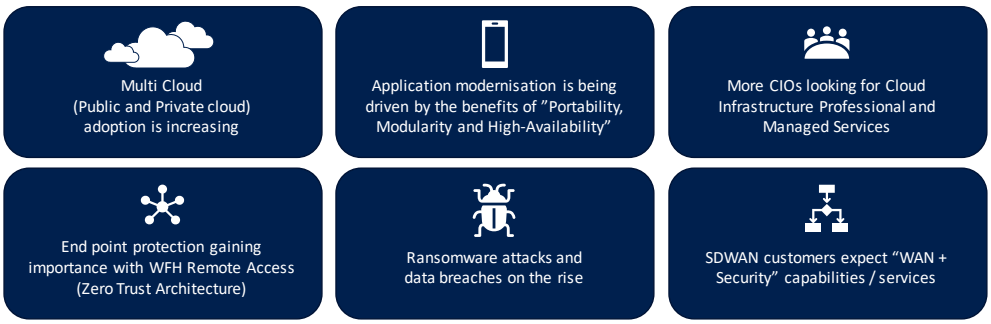
To us, it is encouraging to see Clavister being capable of delivering complete security suites to new innovations launched by world class Service Providers like Telco.

Tata Communications

Clavister has partnered with Tata Communications, which is a global leader in digital connectivity through its managed services and cutting-edge infrastructure. Tata carries around 30% of the world's internet routes and connects businesses to 60% of the world's cloud giants and 4 out of 5 mobile subscribers. Its capabilities are underpinned by its global network, a Tier-1 IP network with connectivity to 200 countries and the world's largest wholly owned subsea fibre backbone. It serves 7,000 customers globally, and over 300 of the Fortune 500. Its offerings include global connectivity services, collaboration and connected solutions, and cloud, hosting, security, and SD-WAN. Unlike Telco, Tata does not offer pre-defined solutions to its customers. Instead, solutions are designed for specific customer's needs. According to Clavister, its partnership is currently entering commercialisation.

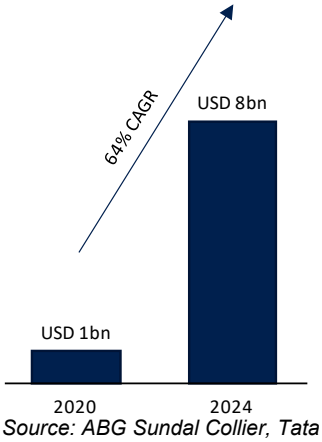
At its recent Capital Markets Day, Tata provided an overview of the most important current market trends as well as the market potential it sees for its offerings. We have highlighted some of the information that is relevant to Clavister. Cloud migration and security seem to be the overarching themes with customers looking for more outsourcing of infrastructure (Multicloud, Managed Services etc.), and more complete solutions that incorporate security at its core (SD-WAN or even SASE solutions that incorporate more sophisticated endpoint protection and Zero Trust Architecture). Our assessment is that Clavister is well positioned to help Tata and other Service Providers deliver these kind of solutions. Interestingly, Tata forecasts that the global market for SD-WAN solutions will increase 7x from 2020 to 2024, which bodes well for security providers like Clavister.

Market trends



Source: ABG Sundal Collier, Tata Communications

SD-WAN offering

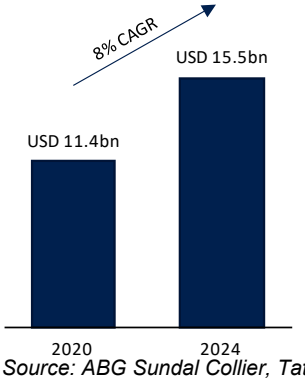


The Opportunity

"Globally – 60% of customers choose a Managed Service Provider for their SDWAN requirements, where we have developed strong capabilities"

Source: ABG Sundal Collier, Tata Communications

Managed Security Services



The Opportunity

- **"Enterprise risk**: Solutions for ransomware attacks, data breaches, etc.
- **Security embedded** in network transformation
- Increased **adoption of analytics** to handle advanced zero-day threats
- Heightened **cloud security**
- Privacy and **Regulatory compliance** pressures"

Source: ABG Sundal Collier, Tata Communications

"SASE represents the future of network security" - Gartner

SASE (Secure Access Service Edge)

According to Gartner, SASE solutions represent the future of network security in the cloud by addressing the most common security challenges of today[15]. Challenges that arise from more applications living outside the data centre, sensitive data being stored across multiple cloud services, and users connecting from anywhere and on any device. Clavister expects to launch its own SASE solution in H2'21. Several US firms have already launched SASE solutions. But as far as we know, no other EU-based firms have.

SASE in a nutshell

Secure Access Service Edge is a concept coined by Gartner that combines multiple technologies into a single fully integrated cloud offering, providing enterprises with a single pane of glass overview of their network. The goal is to offer secure network services anywhere the user connects in from. As workload and users have become distributed, enterprises find themselves having to deal with multiple technologies that do not necessarily work together. This means multiple security policies and inefficient design that are costly and do not scale. With the increase of work from home users, there is a bigger demand than ever for secure direct access to the cloud without having the central bottleneck and latency of the traditional VPN. SASE attempts to solve this problem by combining Security as a Service, with Network as a Service. Gartner has laid out a framework for the core applications needed. These include: SD-WAN as the networking solution, Secure Web Gateway (SWG), Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA).

The future of enterprise networking

Most enterprises are not prepared to abandon their legacy infrastructure. But as the cloud migration continues, they will look to complement the SD-WAN infrastructure with SASE. Then, enterprises get a solid on-site solution with good communication between sites, with security functionalities on-site. On top of this, they get cloud-based services that complement the on-site security as well as provide security for remote workers. Over time, Clavister expects that its SD-WAN and SASE offerings will become fully integrated into one offering. Today, customers can already get a SASE-like solution by complementing Clavister Secure SD-WAN with Clavister Elastic Cloud.

Primary business benefits according to Cisco:

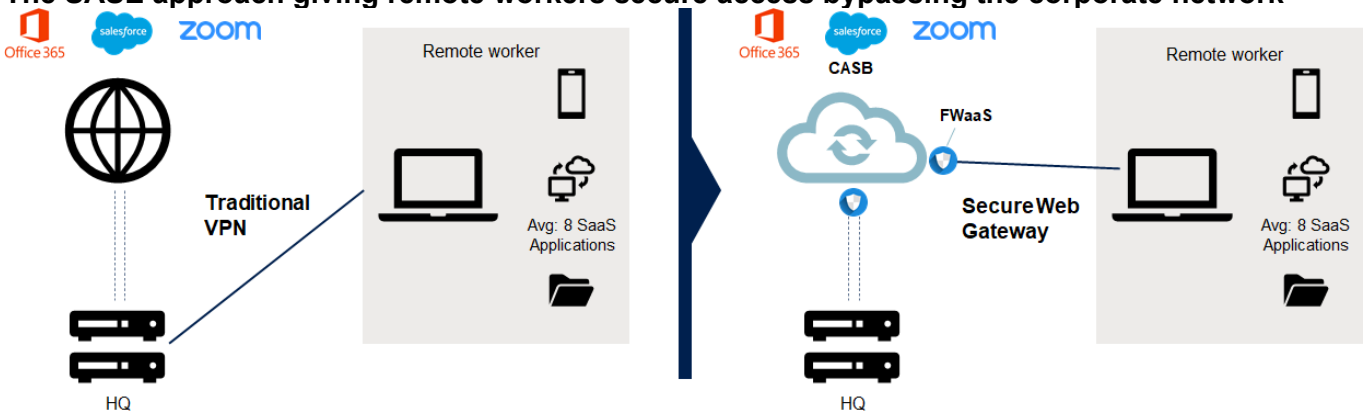
- Reduced costs and complexity
- Enable secure remote and mobile access
- Provide latency-optimised policy-based routing
- Improved secure seamless access for users
- Improved security with consistent policy
- Update threat protection and policies without hardware and software upgrades
- Restrict access based on user, device, and application identity
- Increase network and security staff effectiveness with centralised policy management

[15] The SASE framework has been designed and developed by Gartner as an industry standardisation

A SASE approach is fundamental in the age of remote working

SASE solves a major problem that has emerged from the surge of remote working – users having to be routed through the corporate network to access Internet services in a secure way. Surging volumes of remote workers may cause latency issues for users trying to connect to a secure VPN. By providing a Secure Web Gateway for users to access SaaS applications, enterprises reduce the risks of users bypassing the security perimeter of the corporate network. A Cloud Access Security Broker (CASB) is cloud-hosted software or on-prem software or hardware that acts like a intermediary between users and cloud service providers. CASB has become an integral part of enterprise security, allowing organisations to safely access the cloud while protecting sensitive data.

The SASE approach giving remote workers secure access bypassing the corporate network

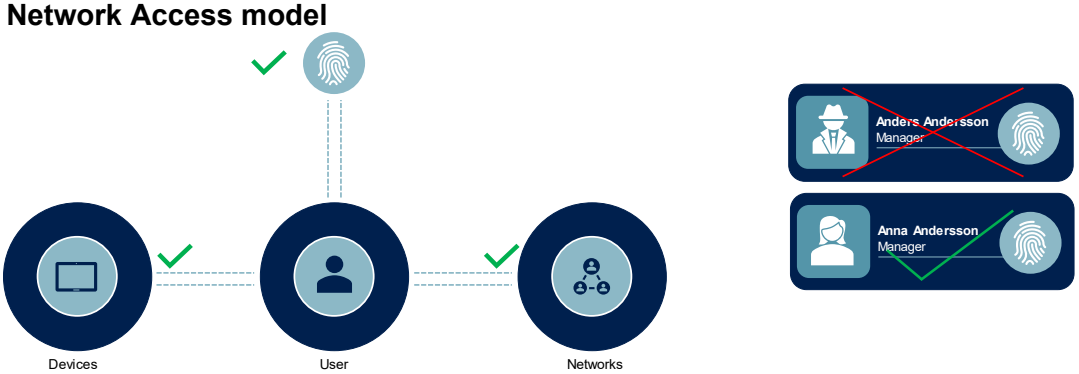


Source: ABG Sundal Collier, CICO

Zero Trust Network Access (ZTNA) is a core principle in the SASE concept

Trust no one, verify everyone. That is the principle SASE is built on. ZTNA is the identification and authentication mechanism that allows a user to access a resource, no matter where they are connecting in from. In a nutshell, the zero-trust model means that no application is regarded secure – opposite to the traditional model where the corporate network functioned like castle protected by firewalls, where every application inside the castle is considered secure. For access to be given to an application in the zero-trust model, the user and the application always needs to be identified and verified by the system. If users are off the corporate network (i.e. a remote worker) the client connects them to the nearest pop location where security services inspect and route them accordingly. If they are behind the corporate network (i.e. the SD-WAN), the SD-WAN steers them where they need to go and offloads a security inspection when necessary.

Zero Trust Network Access model



Source: ABG Sundal Collier, Okta

Gartner expects wide adoption of SASE infrastructure
Gartner expects enterprises to adopt SASE by gradually shifting from traditional network management and security. In 2025, they believe that at least 40% of enterprises will have explicit SASE strategies, up from 10% in 2020 and 1% in 2018. They will start by consolidating the number of security vendors and phasing out on-prem hardware in favour of cloud-based delivery of SASE capabilities. With that said, we expect that Clavister will continue to develop its SASE platform and transition its Secure SD-WAN users into the SASE platform as the market matures and Clavister's offering becomes more comprehensive.

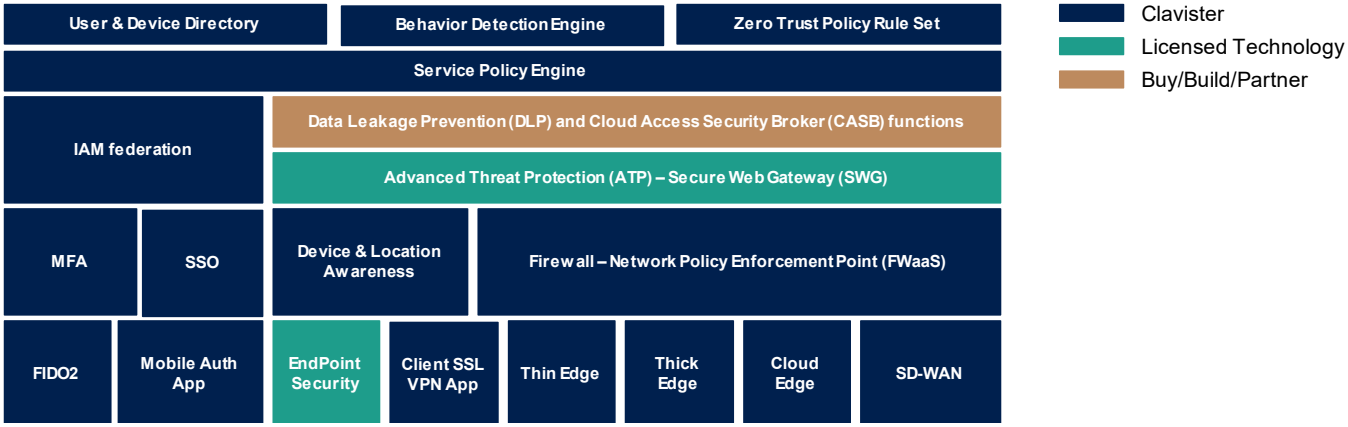
SASE enables further scale up of less expensive bandwidth
As SASE utilises SD-WAN as a critical networking component, it will benefit from more cost-effective and efficient broadband. According to Gartner, 30% of enterprises will have an internet-based WAN connection only (opposite to private MPLS or DSL lines), by 2023 vs. 10% in 2020. Moreover, a transition to SASE eliminates the dependence on hardware appliances to secure the network, as all security functionality is available in the cloud (Authentication, FWaaS, anti-virus etc.).

SASE could lead to a consolidation in the cybersecurity space
The basic principle of SASE is to consolidate networking functionalities with security, and identity and access solutions, providing enterprises with a one-stop-shop for networking a security. To be able to offer a SASE solution, a lot of functionalities are needed, which will most likely result in a consolidation of security vendors. Gartner expects that the percentage of enterprises that source all their base security solutions from one single vendor will increase from 5% in 2019 to 20% in 2023. As far as we now, Clavister will be the only firm in Europe to complete a SASE offering on the market, putting it in an advantageous position to lead the consolidation in Europe.

Clavister SASE – Based on 75% proprietary technology

Clavister expects to launch its SASE solution in H2'21 to the initial target group, public administrations in Sweden, and later scaling it to the Nordics and the rest of Europe. The solution will also be offered to OEMs and Service Providers. One of the key strengths of the offering is that Clavister owns more of the tech stack than most other vendors, which will drive high margins and allow for good flexibility in licensing agreements. According to the company, most of the competitors offering SASE solutions are to a large extent just integrators of third-party solutions. More on the positive side is that Clavister will be able to leverage its strength in Identity Management as identity is at the core of SASE. On the negative side, according to us, is that Clavister is missing some of the core functionalities of SASE – Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB).

75% proprietary technology puts Clavister SASE at an advantage vs. the competition



Source: ABG Sundal Collier, company data

"[Firewalls] remain the ideal control point in an enterprise, serving as the first line of defence"
– Palo Alto Networks

New security solutions, like SASE and SD-WAN, builds on Next Generation Firewalls

Next-Generation Firewall solutions

Network firewalls are one of the primary ways for perimeter protection. They monitor and control incoming and outgoing network traffic. Places for firewall deployment have increased with the Internet broadening corporate networks. Next Generation Firewall (NGFW) solutions are both virtualised and appliance based to provide peace of mind for every corner of corporate networks. According to Palo Alto Networks, a world leading NGFW provider, today's security solution needs to start with the NGFW as the foundation. A NGFW – deployed in physical, virtual, and cloud forms and powered by cloud-delivered security services – remains the ideal control point in an enterprise, serving as the first line of defence[16]. Several of Clavister's solutions (i.e. Secure SD-WAN, SASE, and 5G Security) builds on its NGFW product (Clavister NetWall) as a core part of the offering.

Security by Sweden – Firewall guaranteed without backdoors

Clavister Next Generation Firewalls are made in Sweden completely in-house on proprietary technology. This full control enables Clavister to guarantee that its NGFWs are 100% backdoor-free, and not vulnerable to the flaws that are periodically found in operating systems like Windows and Linux. With mounting geo-political tensions, the value proposition of a firewall provider guaranteed without backdoors can increase significantly. And looking at its international peers, many have been affected by backdoor bugs in the past (see table below) – which Clavister says is much harder for its solutions. We view Clavister's high level of proprietary technology as a significant moat, which is clearly demonstrated in this table.

Many other vendors have been affected by backdoor bugs

	Heartbleed	Shellshok	Ghost	Freak
Barracuda	●	●	●	○
Checkpoint	●	●	●	○
Cisco	●	●	●	●
Clavister	○	○	○	○
Cyberoam	●	●	—	○
Fortinet	●	●	●	●
Juniper	●	●	○	●
Palo Alto Networks	○	●	●	○
Securepoint	●	●	●	—
Sophos	●	●	●	●
Watchguard	●	○	●	○

○ No firewall affected ● All firewall affected ● Some firewall affected
● All firewall affected but cannot be attacked according to vendor — No information

Source: company data
Disclaimer: Statement valid at time of attack publication. Vendors might have patched their products since.

[16] https://start.paloaltonetworks.com/4-key-elements-ml-powered-ngfw.html

Clavister NetWall protects the perimeter
Clavister NetWall monitors and controls incoming and outgoing network traffic. It provides integrated threat protection in several forms: Untrusted traffic can be scanned for viruses and malware. All email and web traffic specifically get thoroughly screened for known threats and behavior. For example, email attachments are always screened as well as email links checked.

Restrict access to inappropriate content and compliance with regulations
There are several reasons why certain web sites might have to be restricted, both for compliance reasons and to restrict an employee's usage of non-business web browsing to gain efficiency. If 100 employees save one hour a week, savings can amount to over EUR 100,000 per year. For both enterprises and SMEs, it could have a significant impact on the bottom line, not to mention savings from avoiding embarrassing situations and punishment from non-compliance behavior.

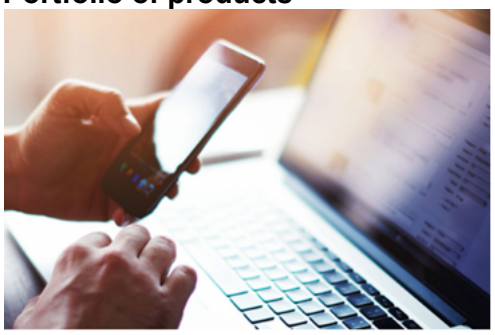
Active traffic optimisation
On the border of the network, Clavister NetWall acts as a policy gatekeeper, prioritising different types of traffic. Virtual pipes can be created to manage different traffic sets, with user identification to make decisions on what traffic pipe a particular session belongs to. For instance, voice and video calls will have higher quality and less interruptions, while file syncing applications like Dropbox will be deprioritised and just take a second or so longer to sync the files in the background, but continue to operate as normal.

Clavister Multi Factor Authentication solution is used by many critical government institutions in Sweden

Identity and Access Management

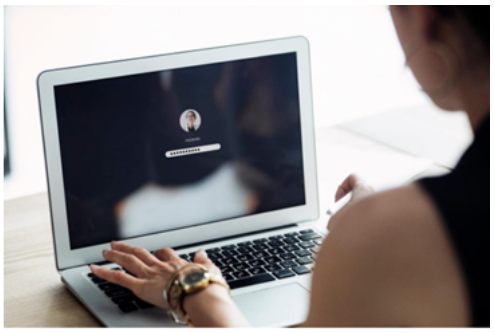
Identity and Access Management (IAM) is a solution that can be offered on a standalone basis or included in other offerings, to organisations that want to ensure the authenticity of its end-users. The Clavister IAM portfolio consists of products that allow enterprises to manage and secure identities of their users as well as securing accounts with valuable information.

Portfolio of products



Clavister **Easy**Access

Increasing security while adding simplicity – saving time for both users and administrators



Clavister **Easy**Password

Reducing IT support costs while improving end-user experience

Source: company data

Solution – Multi factor Authentication or 2-Factor Authentication

Users are typically not careful enough with passwords – not using a wide enough variety of characters. Today, passwords without combinations are solved pretty much instantly by hackers. Multi Factor Authentication (MFA) provides an easy and secure way for users to log in. Clavister's MFA is used by many critical government institutions in Sweden. It is a solution that improves security and makes it easy for an administrator to know who is logged in as the intended user. With Flexible Remote Access integration, users are empowered to work from anywhere in a secure way.

Time it takes a hacker to 'brute force' a password

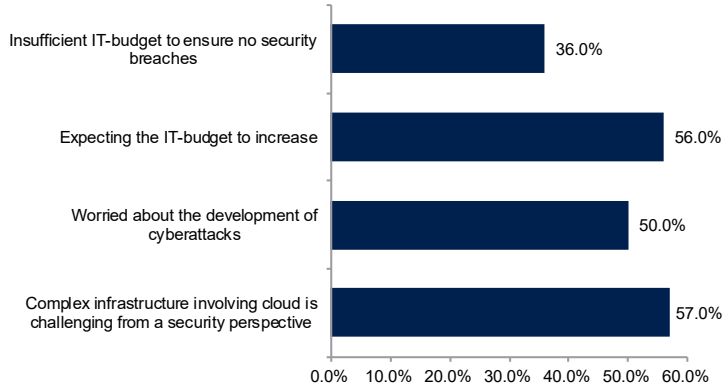
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Source: Hive Systems

Significant potential for Identity and Access Management solutions
According to Mordor Intelligence, the use of traditional authentication methods is challenging the growth of cybersecurity. Their research indicates that over 80% of companies still use usernames and passwords as exclusive means of logging in. To us, this indicated a lot of untapped potential for identity and access management (IAM) solutions, which includes multi-factor authentication (MFA). Moreover, the US government agency NASCIO claims that only 14% of US states have implemented enterprise IAM solutions, while it is a top three (up from no. 5 in 2019) technology and application priority according to its 2021 State CIO Top 10 Priories study[17]. We find it encouraging that governments are taking cybersecurity seriously and see significant potential for solutions like IAM that still have low adoption.

A report by Kaspersky Lab shows that CIO's do not get the support required from top management to handle security issues, and that CIO's in general are intimidated by the threats and security challenges businesses are facing[18]. Around 40% of the CIO's surveyed said that their IT budget is insufficient to protect the organisation from data breaches. In our view, this is unsustainable in a world of increasing levels of data protection regulations (like GDPR) that threatens organisations with hefty penalties for data compromises.

Kaspersky Lab IT Security Officer survey



Source: Kaspersky Lab

[17] https://www.nascio.org/wp-content/uploads/2020/12/NASCIO_CIOTopTenPriorities.pdf
[18] https://www.securityuser.com/se/Nyheter/Samhalle/86-av-it-sakerhetscheferna-gar-inte-att-undvika-dataintrang1

Cyber Armour

Militaries around the world are running modernisation programs, digitalising vehicles, vessels, aircraft – with all of them in need of cybersecurity. Historically, heavier guns have been met with thicker armour. But what happens if the armour is penetrated by a cyberattack? Clavister offers a wide range of products and services to military agencies and OEMs, including solutions for authentication, SD-WAN solutions, and customised products that are embedded in military vehicles. As a security vendor trusted by governments and proven in its field, Clavister aims at leveraging its experience gathered from other industries and offering competitive solutions for the defence industry. With most of the competition in this space primarily focused on defence, Clavister brings new perspective into this market from its experience working with governments and enterprises. We see the design win secured with BAE Systems last year as encouraging, and a testament to its competitiveness in this space. Its first end-customer contract with BAE Systems is worth SEK 50m to Clavister, and we expect more to come as all new military vehicles are mandated to carry embedded cybersecurity solutions by 2024.

Modernisation in the military is changing the playing field

During the Ukraine conflict, conventional military operations were combined with cyberattacks that infected android applications used by Ukraine forces for artillery targeting, GPS jamming and spoofing. For a cyberattack to achieve its desired impact, like making a vehicle halt or reduce its capabilities, its likely to be in the form of weaponised malware. Militaries around the world are responding by running modernisation programs, digitalising vehicles, vessels, aircraft – with all of them in need of cybersecurity.

Cybersecurity will be mandatory on all new vehicles from July 2024

New UN regulations on cybersecurity has made the European Union decide to make cybersecurity mandatory on all new vehicles produced from July 2024[19]. This new regulation is aimed at tackling emerging risks associated with the digitalisation of in-car systems. According to the UN, cars today contain up to 150 electronic control units and about 100m lines of software code (expected to reach 300m by 2030). This comes with significant cybersecurity risks as hackers that get access to electronic data and systems may threaten vehicle safety and consumer privacy. This regulation goes for military vehicles as well, a segment Clavister has identified as an attractive area for its products to be deployed.

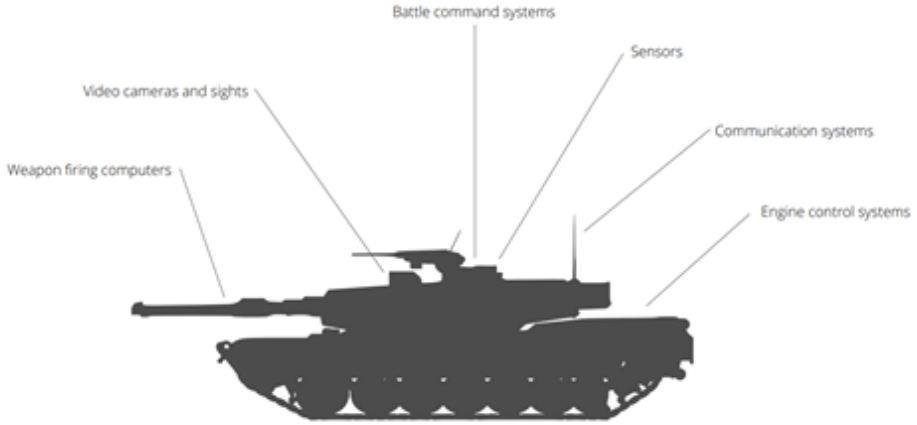
What Clavister brings to the table

As most of its competitors are focused primarily in the defence industry, Clavister is able to bring new perspectives from its experiences in other industries where the security challenges look quite similar. The company is a proven provider of security solutions for mission critical government agencies. As a Swedish firm with proprietary technology it is more independent than many of its competitors – firms with connections to countries that are reported to be weaker on data privacy and protection. Furthermore, it creates synergies as Clavister can use its existing technological platform to design solutions specifically for deployment in the defence space. What's more is that Clavister is proven in this field. It has been working with defence OEMs and system integrators for years before making it an official strategic priority.

[19] https://unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

Examples of well-known weaponised malware used by military forces
Two well-known examples of weaponised malware are Stuxnet, which was used to sabotage Iranian nuclear centrifuges, and BlackEnergy, which caused a power outage in the Ivano-Frankivsk region in Ukraine in December 2015. A weaponised malware is a dangerous weapon as it can spread from one system to another, cover its tracks, and fly under the radar by dynamically changing itself to avoid detection. The more connected vehicles get, the more vulnerable they are. What was special with Stuxnet was that it was designed to look for PLCs – small computers that control things like factories, power grids, and nuclear plants[20]. The Iranian power plant was not connected to the Internet. So, to reach its target, the malware travelled through devices until someone brought it inside the secure facility via a USB stick, by accident. This shows that every system or network is vulnerable.

Every military vehicle needs embedded cyber defence



Source: ABG Sundal Collier, company data

Case study - BAE Systems
BAE is Europe's largest defence contractor and the world's third largest. Its subsidiary Hägglunds, produces vehicle systems for military and civil applications. Key products include Combat Vehicles and Armoured All-Terrain Vehicles. The latest versions of these two are integrating Electronic Architecture NATO standards, which drives the demand for cybersecurity. Clavister is contracted to deliver a military-graded security gateway and secure switch into the two vehicles.

The first end-customer contract is for a Western-European military organisation, worth SEK 50m to Clavister, with a potential of up to SEK 90m. Subsequent contracts would be worth SEK 20-100m each for Clavister. With this design win, we believe that Clavister is likely to be awarded more contracts going forward.

The requirements for this kind of equipment is obviously higher than equipment intended for datacentres etc. as the equipment needs to be resistant to not only cyberattacks, but the physical environment as well.

But also, these vehicles are basically becoming datacentres on wheels (tracks), containing over 50 different computer engines, with weapon firing computers, video cameras, battle command systems, sensors, etc. – all being integrated and potentially sensitive to cyberattacks.

[20] According to Symantec.

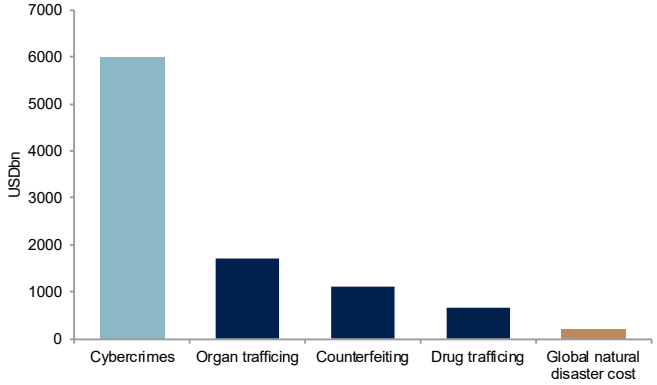
Cybercrimes: a major problem

Cybercrimes are a large and expanding problem for both enterprises and society. Economic damages related to cybercrimes are expected to reach USD 6.0tn in 2021, and are growing at 15% p.a. The total cost of cybercrimes exceeds that of organ trafficking, drug trafficking and counterfeiting combined.[21] Ransomware is one of the fastest-growing cybercrimes and can leave a company paralysed for weeks by denying access to files, systems or networks. Due to the sensitivity of their operations and potential impact on healthcare and other critical infrastructure, public administrations (one of Clavister's core customer segments) have become one of the most common victims of hackers. We believe that enterprises and public administrations will be forced to increase cybersecurity spending significantly in the coming years.

Cyberattacks are increasingly intensive and damaging

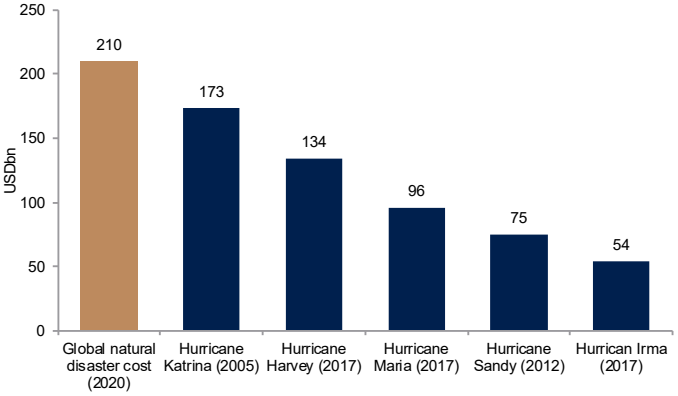
Organisations and government agencies around the world are taking action to secure critical networks (such as 5G), as network failures can have lethal consequences. Outages can lead, for example, to cities going dark, production shutdowns, national economic catastrophes, medical emergencies and accidents as the systems that govern our lives fail. Both the frequency and intensity of cybercrimes have increased over the last decade, resulting in huge losses for businesses.[22] Cybersecurity Ventures expects global cybercrime-related costs to grow by 15% p.a., reaching USD 10.5tn annually in 2025 (vs. USD 3tn in 2015 and USD 6tn expected in 2021).[23] The damage inflicted on the global economy trumps all damage from natural disasters, as well as the global trade of all illegal drugs combined.[24] Included in these calculations are the destruction of data, stolen money, lost productivity, theft of intellectual property and more. The US Federal Bureau of Investigation warns that every American citizen should expect that all of their personal data has been stolen and is available on the dark web.[25]

Damage from cybercrimes vs. the retail value of other transnational crimes



Note: Cybercrimes (2021e), Other crimes (2017), Natural dis., (2020)
Source: ABG Sundal Collier, Global Financial integrity, Cybersecurity Ventures.

Damages of the most expensive natural disasters in US history, and global costs in 2020



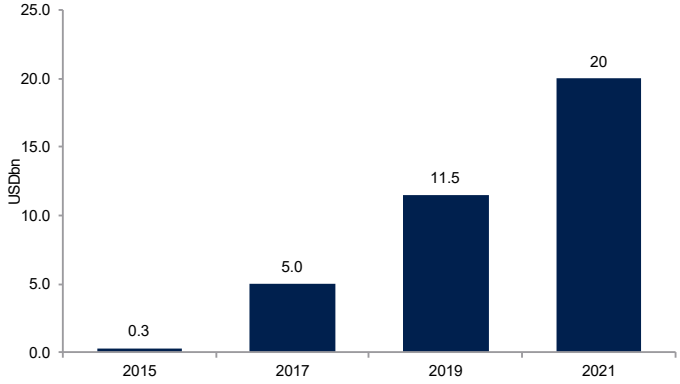
Source: ABG Sundal Collier, Statista, Munich Re.

[21] According to Cybersecurity Ventures
[22] According to Cybersecurity Ventures
[23] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[24] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[25] https://www.wsj.com/articles/what-happens-to-your-data-after-a-hack-1544367600?mod=hp_lead_pos10

Cybercrimes

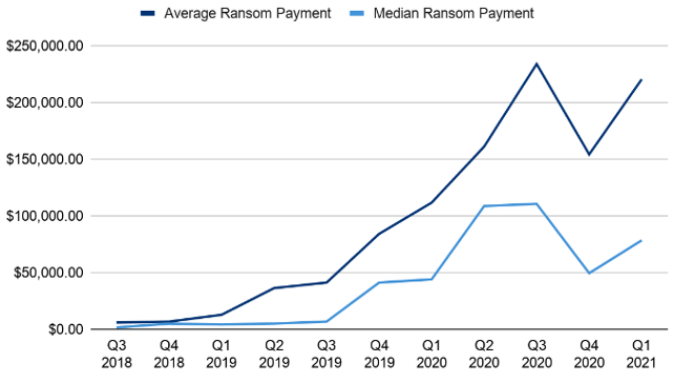
Among the most common kinds of cyberattacks are ransomware attacks, hijacks, DDoS (dedicated denial of service), malware attacks and data breaches. Ransomware has become one of the biggest risks to company operations and is regarded as the “go-to method of attack”, according to the US Department of Justice.[26] Ransomware is a form of malware that infects computers and mobile devices, restricts access to files and may threaten permanent data destruction unless a ransom is paid. On average, attacks leave companies paralysed for 23 days (Q1’21 numbers, +10% q-o-q), according to Coveware. This is not only one of the fastest-growing crimes, it is also one of the most damaging to both businesses and citizens. According to Coveware, both the number of ransomware incidents and the ransom demands themselves have increased. Global ransomware costs are predicted to hit USD 20bn in 2021, up from USD 11.5bn in 2019 and USD 5bn in 2017[27]. The average ransom payment increased by 43% between Q4’20 and Q1’21, to USD 220m (median of USD 78m). The damage this inflicts on a business can be devastating, and when critical infrastructure is targeted, the physical health of citizens is impacted as well. According to Cybersecurity Ventures, ransomware claimed its first life in October 2020, as German authorities reported a ransomware attack that caused the failure of IT systems at a major hospital in Dusseldorf, leading to the death of a woman in need of urgent admission.

Exponential growth in ransomware damages



Source: Cybersecurity Ventures

Avg. ransom payment increasing rapidly



Source: Coveware

What does ransomware look like?

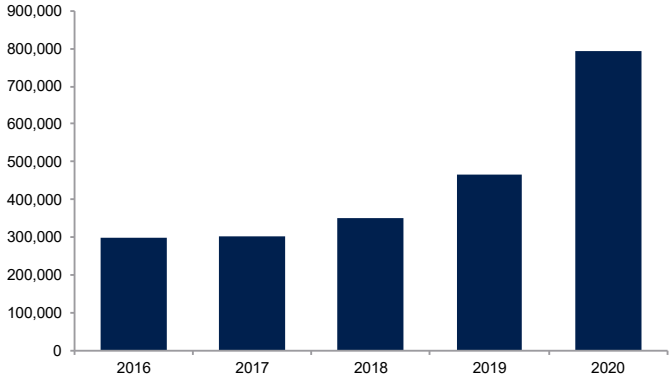
One of the most well-known ransomware attacks was the WannaCry attack from 2017 that utilised a known security gap in Windows, called Eternal Blue. The virus infected computers with ransomware that locked data on the computer and demanded ransom payments in Bitcoin to unlock it. WannaCry hit around 230,000 computers globally and is estimated to have caused USD 4bn in losses.

[26] https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit
[27] https://cybersecurityventures.com/cybersecurity-market-report/

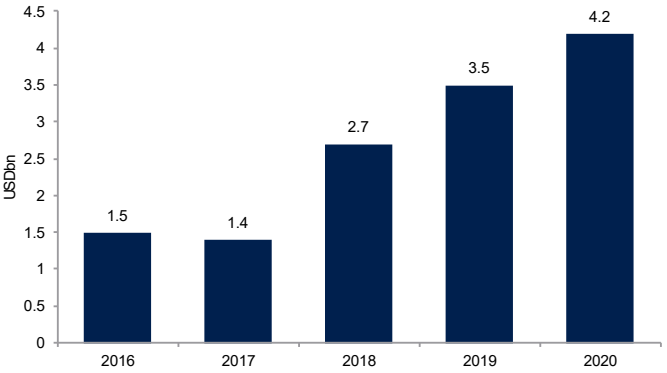
Internet crimes increased 60% in 2020 vs. 2019, according to FBI

FBI's 2020 Internet Crime Report states that worldwide complaints of suspected internet crime reached 792,000 (+60% vs. 2019), with total losses of USD 4.2bn (+70% vs. 2019). While most of the complaints are related to phishing, non-payment/non-delivery and extortion that primarily targets individuals, most of the financial losses comes from attacks targeting businesses (Business Email Compromises/Email Account Compromises, BEC/EAC).

Number of complaints, worldwide



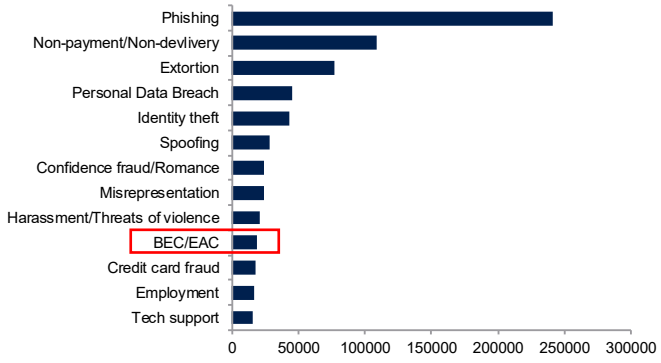
Total losses from Internet crimes (USDbn)



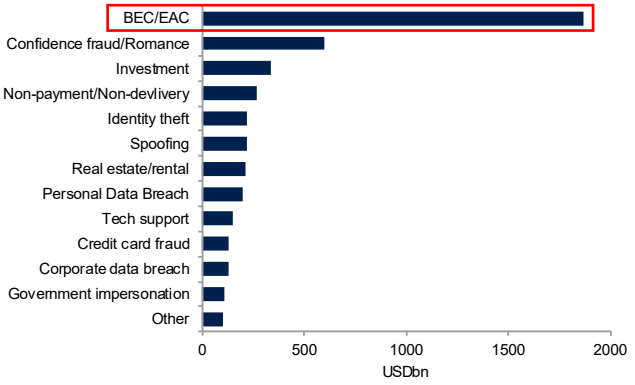
Source: IC3

The most common types of internet crimes are relatively less damaging. Malware that gets into businesses networks via Email accounts (BEC/EAC) is less common but generates most of the losses.

Most common crime types (# of complaints)



Losses per crime type (USDbn)



Source: IC3

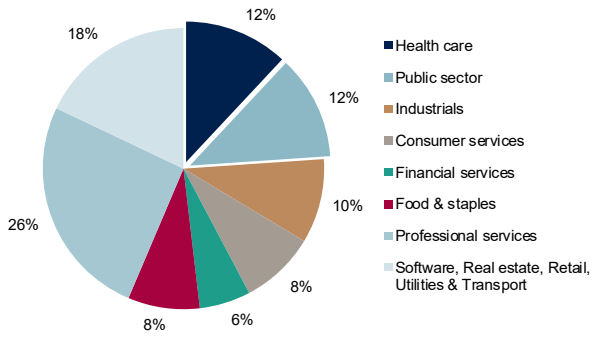
Cyberattacks put pressure on public administrations

Cyberattacks can do more than harm businesses, they can endanger lives. Threats of attacks on critical infrastructure like healthcare providers and first responders puts pressure on states to provide public services with sufficient protection. According to Northwell Health, healthcare is and has been the no.1 priority for cybercrime because of the value of the data that can be obtained and the fact that the criminals know that if they lock up the systems, it has a significant impact on operations because MRI machines and ventilators run on software.

Attacks against municipalities could cause cities to shut down critical infrastructure like communication services, electric utilities, and traffic systems. Research from Barracuda Networks indicates that 44% of all global ransomware attacks in 2020 targeted municipalities. In Sweden, where about a third of public employees worked from home more than 50% of the time in 2020, workers were forced to use private internet connections most of the time.[28] To us, this indicates significant potential for secure access and connectivity solutions: solutions provided by Clavister.

Healthcare and public sector, two of the industries most targeted by ransomware attacks

Share of ransomware attacks in Q1 2021



Source: Coveware

[28] https://www.dagenssamhalle.se/styrning-och-beslut/kommunpolitik/sakerhetsriskerna-har-flyttat-hem/

Growth opportunities

The most important trend that drives demand for the security solutions provided by Clavister is digitalisation. With more services moving online, businesses adopting hybrid-cloud infrastructures, and the emergence of 5G, communication network's interaction with the Internet is now increasing rapidly, making both individuals and organisation more vulnerable. More connected devices, increased complexity of networks as well as the interaction between networks, means that more sophisticated network security and policy control is needed to solve new challenges. In addition, it is our assessment that new EU regulation provides the grounds for prioritisation of EU-based cybersecurity vendors, like Clavister.

Market trends

Digitalisation	Regulation	Adoption of 5G	Complexity	Cloud services	Geo-pollical tensions
The digitalization drives strong demand for identity, integrity and policy control solutions.	The Cybersecurity Act (2019) provides a framework for Europe to become more independent and stay competitive in the cybersecurity space.	Adoption of 5G entails explosive growth of mobile data traffic, thus increasing the need for more sophisticated network security solutions.	Cybersecurity is growing in complicity by the day.	An acceleration of Cloud Services adoption rates creates new network security challenges.	Increased geo-political tensions with the EU lacking its own world-class cybersecurity vendors.

Source: ABG Sundal Collier, company data

EU regulation

The EU Cybersecurity Act (2019) provides the EU Agency for Cybersecurity (ENISA) with a permanent mandate[29]. This makes ENISA stronger, giving it more resources and new tasks, including establishing a framework for EU-wide rules for cybersecurity certification. According to the European Commission, firms doing business in the EU will benefit from having EU cybersecurity certification[30]. The act has demonstrated the need for an EU approach to respond to all challenges, protect the citizens and stay competitive. To succeed with this, ENISA was granted a mandate to provide Europe with the capabilities for cybersecurity research and development, with 5G as a particular priority. Our assessment is that this is an important step towards making the EU more independent and competitive in the global cyber space. The agency will provide financing and a framework to support the development of European-based security, putting Clavister in a solid position as a European leader in cybersecurity. We also believe that Clavister, with solutions tailored for the specific needs of EU administrations and 5G network providers will benefit from this regulation, as most of its competitors are US-based cybersecurity firms. In fact, Clavister has already benefited in several regards. In 2017, Clavister was granted a EUR 20m loan by the European Fund for Strategic Investment. This was an important loan that facilitated the development of Clavister's product portfolio. In addition, Clavister has received funding for joint development projects with partners like BAE Systems from Vinnova, the Swedish innovation agency, which is part of the Horizon Europe project.

[29] https://digital-strategy.ec.europa.eu/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity
[30] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Geo-political tensions

The US-EU Privacy Shield Framework was adopted in 2016. It was designed to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the US to support transatlantic commerce. However, the framework was invalidated by the Court of Justice of the European Union in July 2020. This creates new challenges for organisations cross-border data transfer. According to EY, an organisation should expect increased scrutiny by EU Data Protection Authorities and be ready to demonstrate how privacy controls are designed, and show compliance with all aspects of the GDPR[31]. An important take-away is that an EU-based organisation is responsible for ensuring adequate safeguards when transferring data. Thus, we believe that both service providers operating in Europe, and EU administrators will reconsider their security vendors and to a higher degree opt for EU-based vendors that provide compliance with EU regulations. As Clavister primarily competes with US vendors, this plays right into their hands.

Cloud services and 5G

As the adoption of cloud services accelerates, this entails more entry points into a business' private network. The same goes for 5G networks. Businesses and network providers need to respond by securing the edges of the network by providing a secure connection, and providing identity and access control solutions to every part of the organisation. This requires more advance cybersecurity solutions than the traditional firewall solution. But on-premise security solutions still constitute ~60% of the market, showing that organisations still prefer to keep confidential data in-house, as opposed to handing it over to cloud providers[32]. This indicates that there is still a long runway for secure SD-WAN and SASE solutions that secure hybrid-cloud WAN structures. With infrastructure protection solutions being the dominating type of security solution, with ~27% of market revenues[33], the transition from on-prem to cloud offers significant opportunities for Clavister solutions that are catering to network providers. In addition, we estimate that the penetration of 5G is currently in the mid-single digit range, providing a lot of growth opportunity for Clavister's 5G security solutions.

[31] https://www.ey.com/en_gl/consulting/how-the-nist-privacy-framework-can-help-you-better-manage-risk
[32] According to Grand view research
[33] According to Grand view research

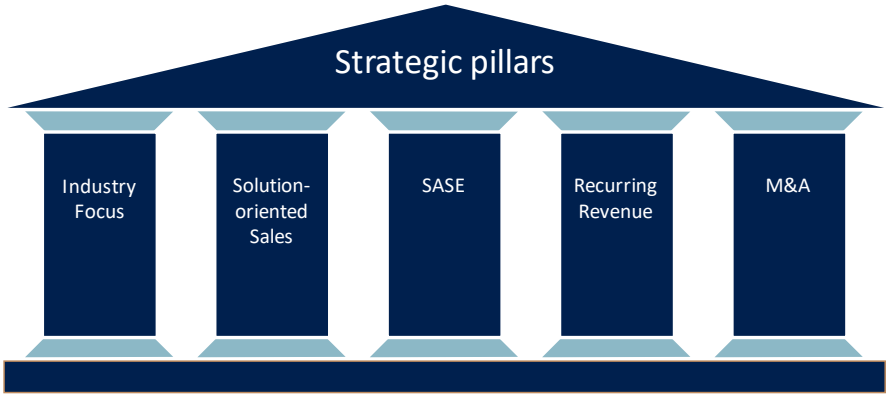
Strategy

Over the years, Clavister has developed a competitive solution portfolio while establishing solid relationships with system integrators and service providers. But strategic execution has been poor. The new strategy from 2018 aims at leveraging the portfolio and the established partnerships to drive growth and scale the business. The growth strategy is based on five core pillars: 1) Consolidate its industry focus to three main industries. Clavister has transitioned from a "shotgun approach" to only targeting industries where it has experienced that its solutions are competitive and attractive to customers. 2) Package its products into solutions that solve specific industry challenges. 3) Develop a SASE solution to future-proof the enterprise offering. 4) Change the revenue model from perpetual licenses to recurring revenue. 5) Complementary M&A. We believe that the main reason for an acquisition would be to strengthen its SASE offering and further reduce the share of third-party licensed software in the solution.

The company has seen several benefits from the strategic shift

Since the strategic shift in 2018, the company has seen several benefits: 1) A clearer and crisper positioning. The company is not seen by customers as a multifaceted and multi-product technology company anymore. 2) Increased viability in the portfolio. R&D efforts can be focused on specific areas instead of developing products in a standalone manner. 3) The ability to attract large accounts has increased, which is an important growth driver.

Five strategic pillars



Source: ABG Sundal Collier, company data

Industry focus

Clavister has found that Service Providers, EU Public Administrations and Defence contractors represent the best scaling opportunities for the company. A more focused sales force frees up capacity to focus more on up-sell and new customers.

Solution provider

Since 2018, Clavister has implemented a new strategy where it packages its security products into pre-defined solutions that cater to specific challenges of the aforementioned customer segments.

SASE

Clavister is putting a lot of effort into its SASE solution to future-proof its enterprise networking offering. Gartner expects that SASE will bring a consolidation in the number of security vendors used by enterprises and Service Providers. Hence, we find it encouraging that Clavister is on its way to becoming a leading EU-based SASE vendor. The solution is expected to hit the market in H2'21.

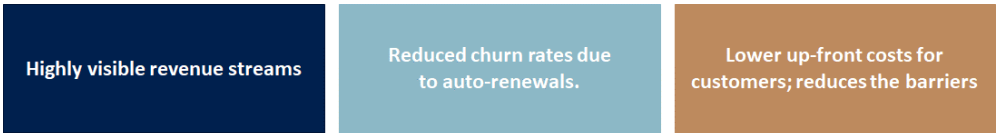
Migrating to a recurring revenue model

An integral part of Clavister's new strategy is its new revenue model that will be rolled out during H2'21. The aim of the new model is to simplify the on-boarding process for the end-user and reducing the up-front investment. Historically, products have been sold on a perpetual license model, with multiple products being sold on different pricing models. This may cause some confusion both for the company and its customers. Now, when the company is shifting from a product selling company to a solution provider, it wants to transition to a term-based recurring revenue model as well.

The company concluded that it will be able to attract more customers with a three-tier pricing model. The company also believes that it would be easier to migrate customers to an advanced solution that is pricier if they start with the base offering.

The main benefits are expected to be: Highly visible revenue streams. Reduced churn rates due to auto-renewals (change from today, where renewals require active decisions). Lower up-front investment for customers (the perpetual license means a big up-front payment from the customer. With the recurring revenue model, the required hardware investment can also be lower as the customer can start with the base offering, which is a light version requiring less hardware investments. As a software company, Clavister does not want hardware – which is used from time to time – to be a deal-breaker for customers to by a solution.

Benefits of the new revenue model



Source: ABG Sundal Collier, company data

M&A

Clavister has made successful acquisitions in the past. In 2016, it acquired PhenixID, an Identity and Access Management solution provider. With the purchase, Clavister was able to diversify its business from mainly offering firewall solutions and strengthening its offering to Public Administrations. As Clavister has embarked on the journey to become a full solution provider, we believe that complementary acquisitions to strengthen its SASE offering will be likely in the future.

Go-to-market strategy

Clavister's go-to-market strategy is based on: 1) working with large accounts such as government agencies or enterprises, and 2) using channel partners (important partners include Nokia, Atea and Tieto) to reach a broad base of potential customers. By going through channel partners, a larger part of the sales organisation can focus on attracting new partnerships or design wins with established partners. This has not always been the strategy. Up until 2018, the focus of the sales organisation was much more dispersed – and importantly, did not use channel partners as efficiently. According to Clavister, going direct to end-users is both more competitive and less scalable than working with channel partners and integrating the solution in large systems provided by Service Providers and defence OEMs, with hundreds or thousands of end customers. We believe that Clavister is well positioned to start scaling up with its partners with no, or very little, addition sales and marketing efforts.

Why is it a successful strategy?
Through its largest partners (e.g. Ericsson, Telco, and Nokia), Clavister reaches all major mobile operators in the world and potentially thousands of enterprises. Thus, the primary focus for Clavister should be to ensure that its technology is up to speed with the latest upgrades of the networking services offered by the Service Providers. And right now, SD-WAN – followed by SASE – and 5G are the emerging technologies, where Clavister can offer a very competitive security offering. A testament to this is Telco licensing Clavister's solutions to secure its new SD-WAN solution as well as Nokia that is reselling Clavister NetShield under its own brand NetGuard[34].

How will Clavister grow?
Clavister will grow by nurturing its relationships with partners and waiting for them to scale up the new network technology (SASE for enterprises and 5G for mobile operators) as Clavister's license fee is based on traffic volumes in the networks. We estimate that Clavister can reach 30% of operators around the world (600-800). Based on estimated revenue per operator (SEK 3-6m, per solution) we estimate an addressable market of ~SEK 800m from just mobile operators[35].

The second growth pillar is for Clavister to attract more EU public administration. With many critical public administrations in Sweden already implementing security from Clavister, we do not see how Clavister will not continue growing in Europe, especially since EU regulation aims at facilitating digital independence, which to us could lead to a de-prioritisation of US-based cybersecurity firms. The third pillar is more defence contracts. We expect that BAE Systems will win more contracts where Clavister's technology is embedded, or that Clavister gets more design wins.

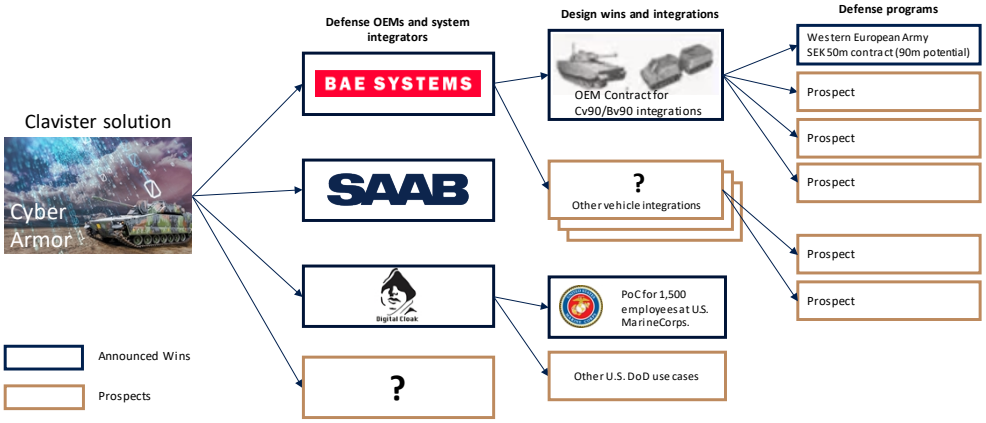
Defence Go-To-Market Model
The Defence go-to-market model differs a bit from Service Providers. It scales through different layers of go-to-market partners. Clavister does not go direct to end users – it is not providing products directly to the armies. Instead, Clavister works with OEMs like BAE Systems and more niched system integrators like Digital Cloak. Through partners, Calvister does system integrations with OEMs that are project based, i.e. Clavister's solution will be sold with each system delivered by the OEM. At the moment, Clavister has two contracts with BAE Systems for two specific vehicles (Cv90 and BvS10). From the integrations Clavister enters various defence

[34] Clavister NetShield constitutes the only virtual firewall solution in Nokia's 5G security offering, NetGuard.
[35] Source: Clavister Business update 07/06/17.

programs run by defence ministries or the respective end-users in the respective countries. This contract with BAE is the first one, with hopefully many more to come.

Clavister's ability to scale comes from: 1) New contracts on this platform (Cv90 and BvS10). 2) New design wins within BAE Systems (within BAE Systems there are many other vehicle systems in need of cybersecurity). 3) Outside of BAE Systems, Clavister has partnerships with SAAB and Digital Cloak, a niched integrator that targets the US Department of Defence and private agencies in the US. Clavister is currently running a pilot project with Digital Cloak to provide identity and access solutions for 1,500 employees in the US Marine Corps. If successful, this partnership will scale with more users in the Marine Corps as well as potentially other use cases within the US Department of Defence. 4) Clavister can sign new partnerships with OEMs and system integrators in the defence space. This constitutes a good example of the high scalability of the go-to-market model.

Defence go-to-market Model



Source: ABG Sundal Collier, company data

Revenue model

Clavister is consolidating its revenue model to a recurring revenue model to help facilitate its strategic changes. It previously had different revenue models that varied depending on multiple factors. Today, the revenue model is being consolidated to a uniform multi-tier as-a-service model, including a base offering that allows for a simple and less expensive onboarding. For some solutions, like the 5G and Defence solutions, the revenue model is a bit different. For the 5G solution, some customers are charged based on maximum data capacity, meaning that Clavister can scale with both the number of subscribers and the traffic volume in the networks. For the Defence segment, the revenue is mostly project-based. With the new revenue model, we believe that Clavister is well-positioned to streamline onboarding of new clients, as well as attract larger accounts that will help drive scale.

Consolidating the revenue model

Source: ABG Sundal Collier, company data

Forecasts

Clavister operates in a fast-growing market. Its ambition is to grow by 20% p.a. and increase its market share. In the near-term ('21e-'23e), we forecast a 19% sales CAGR, mainly driven by the 5G roll-out and the BAE Systems contract. Moreover, we expect that opex will remain relatively flat over the same period, allowing Clavister to scale on its cost base. This should result in positive EBITDA in 2022 and EBIT in 2023. In terms of EBITDA, we forecast '22e-'23e margins of 3% and 16% respectively.

Clavister's ambition is to grow sales by 20% p.a.

Between 2015 and 2020, Clavister grew sales at a CAGR of 15%. Growth in 2019-2021 has been disappointing, in our opinion, but we think that sales have been temporarily impacted by the change in strategic direction set in 2018 as well as the new management team. From a more long-term perspective, we believe that the company has established a strategic foundation to accelerate growth from here. The company has said that its ambition is to grow sales by 20% on average in the coming years.

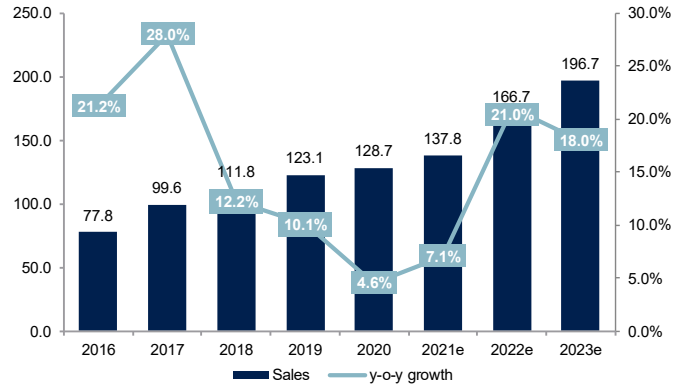
We forecast a 19% organic sales CAGR in '22e-'23e

With 5G penetration expected to continue increasing rapidly, and the company's project with BAE Systems (expected to commence in 2022-2024), we forecast 21-18% organic sales growth in '22e-'23e. We expect that some legacy clients will churn off in the coming years, as the company has redirected its sales efforts to target larger accounts and partners. But we think this will be compensated by the delivery of the BAE contract worth ~SEK 50m, as well as 5G revenue that could grow at 20-40% p.a. in the coming years, according to our research.

Order intake

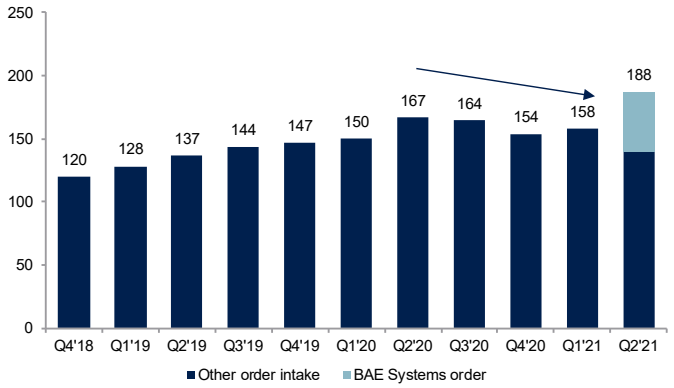
Order intake is a good leading indicator of Clavister's underlying growth. That said, the order intake has showed negative momentum on a R12m basis in recent quarters. We saw a rise in Q2'21, but this was mainly due to the defence contract order that contributed with SEK 48m. Excluding this item, the order intake was lower y-o-y. Our assessment is that the company might be churning out some legacy clients. We have also gotten the impression that 5G revenue growth slowed down a bit in 2021, from growing at a CAGR of +30% from 2017-2020.

Sales and sales growth y-o-y



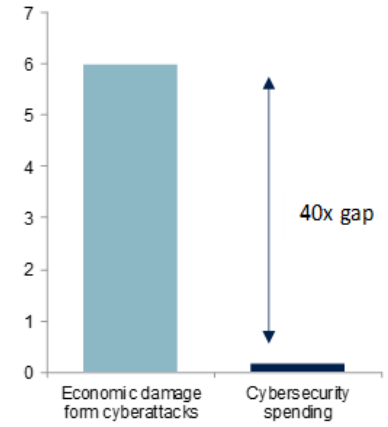
Source: ABG Sundal Collier, company data

R12m order intake



Source: ABG Sundal Collier, company data

Damages are 40x the spending, (USDtn)



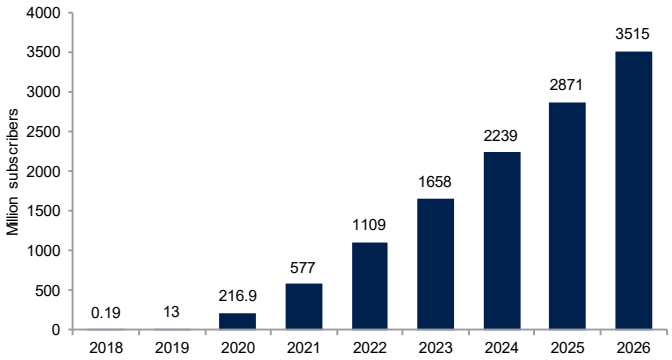
Source: Cybersecurity Ventures, Gartner

Growth drivers

Clavister's ambition is to grow faster than the underlying cybersecurity market, which is expected to grow at ~8% p.a. Clavister's sales mix is tilted towards market segments that we think will grow faster than the total market. Public administrations are still underinvesting in cybersecurity, in our opinion, and thus will need to catch up. There is a giant gap between the scale of cybersecurity damages and the total cybersecurity spending, and we believe that cybersecurity spending will consequently rise.

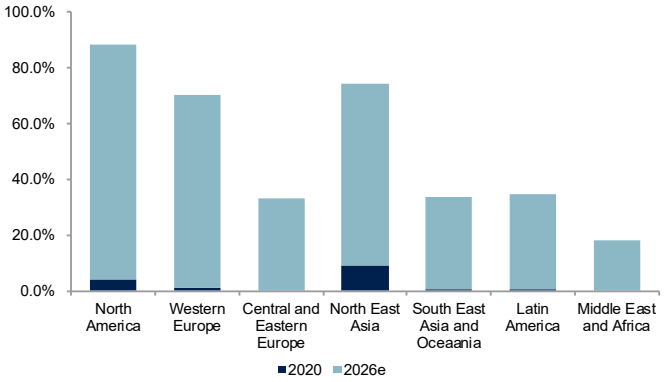
In addition, Clavister has good exposure to the rapidly growing 5G cybersecurity market. According to Ericsson, 5G penetration in Western Europe is expected to increase from 1% in 2020 to 60% in 2026. Importantly, a significant part of Clavister's 5G revenue is based on network capacity. This means that Clavister will be able to grow revenue in proportion to network capacity. We do not expect that its 5G revenue will expand 60x by 2026, however, as we believe there will be some price pressure on the price per unit of data traffic. Nonetheless, we think Clavister could multiple its current 5G revenue many times from current levels. Other important growth drivers include more EU regulation that benefits local players like Clavister, geopolitical tension and digitalisation in general.

Number of 5G mobile subscribers



Source: ABG Sundal Collier, Ericsson mobility report 2021

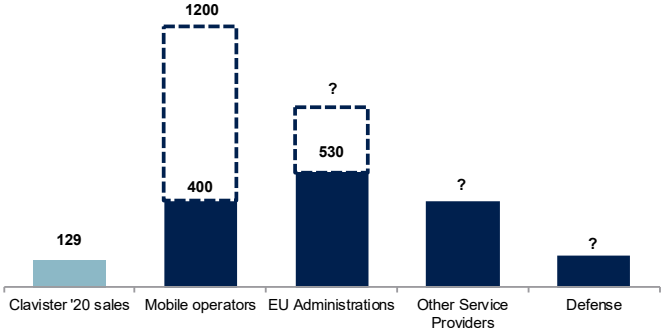
5G penetration per region, 2020 vs. 2026



Source: ABG Sundal Collier, company data

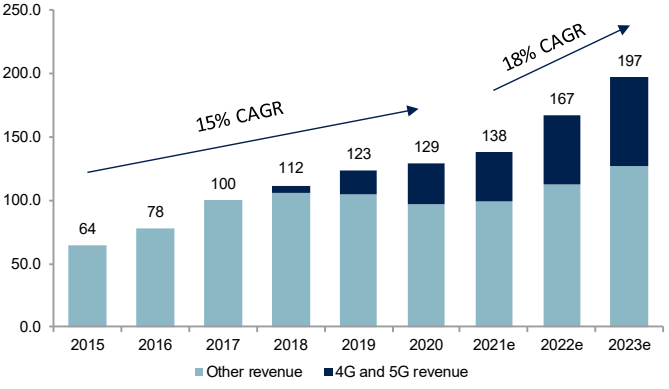
We estimate that Clavister's share of 5G revenue will increase over time to become a more significant share of total revenues, as the firm will be able to partner with more mobile operators. It currently works with ~5% of all global major mobile operators, through Nokia and Ericsson. According to the company, it could potentially reach ~30% of operators. This implies a significant market potential. We estimate the 5G potential to be SEK 400m-1200m in annual revenue for Clavister.

Significant market potential in several verticals



Source: ABG Sundal Collier, company data

ABGSC estimates of 4G/5G revenue

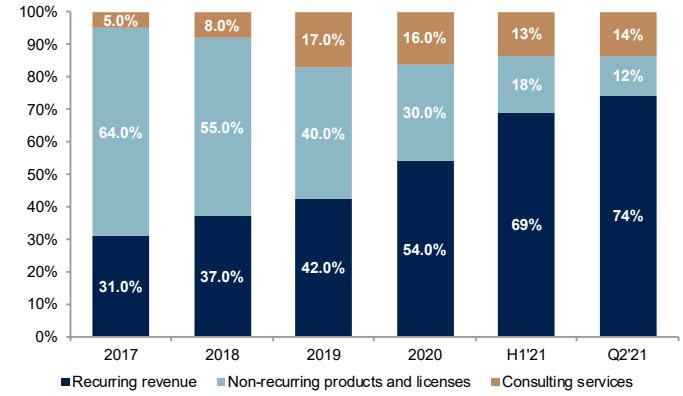


Source: ABG Sundal Collier, company data

High gross margin

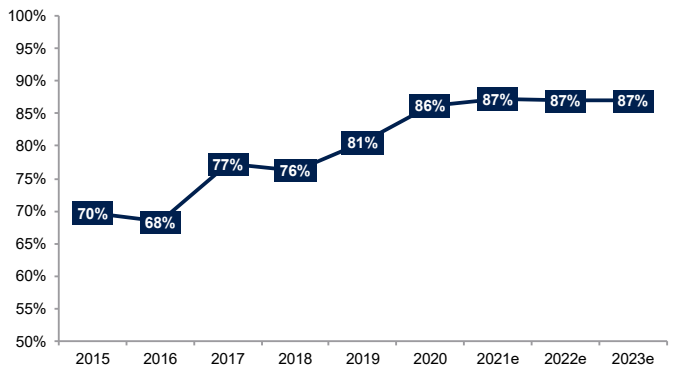
Clavister's higher gross margin has been boosted by a change in revenue mix towards more recurring revenue and less product sales. This change has been accelerated by the introduction of the SaaS model this year. In '22e-'23e ,however, we think that the share of non-recurring and product sales could increase with the roll-out of the defence contract with BAE Systems, which include more hardware. Correspondingly, we think that the positive momentum seen in the gross margin will stagnate due to the change in sales mix. Beyond '23e, however, we see potential for the gross margin to increase once again.

74% recurring revenue in Q2'21



Source: ABG Sundal Collier, company data

Gross margin development

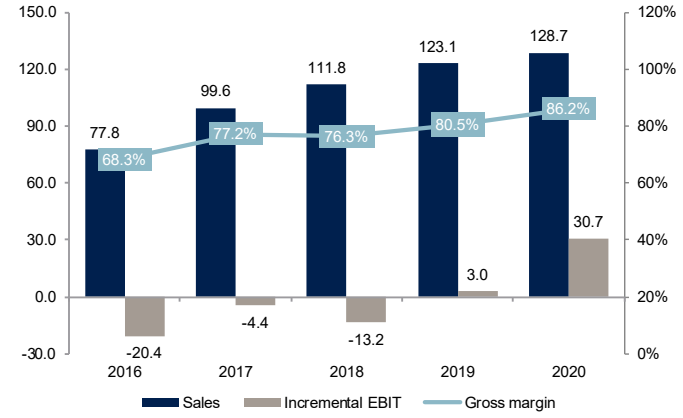


Source: ABG Sundal Collier, company data

Quickly approaching break-even

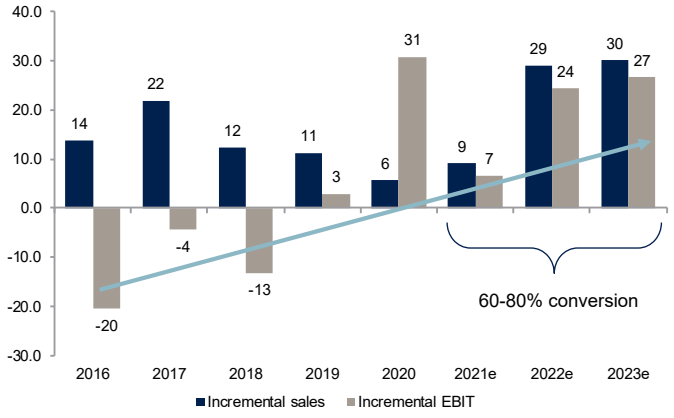
With high gross margins and low incremental opex requirements to drive sales growth, most additional sales filter down to the bottom line. As such, increasing sales volume is the single most important thing for Clavister right now. The incremental EBIT, i.e. the y-o-y increase in absolute numbers, went from negative in 2018, to break-even in 2019 to SEK 31m in 2020. In '22-'23e, we estimate that 60-80% of the incremental sales will fall directly to EBIT, which corresponds to EBIT rising from SEK -49m in 2021 to SEK -14m in 2023.

Positive trend in incremental EBIT



Source: ABG Sundal Collier, company data

High conversion of incr. sales to incr. EBIT

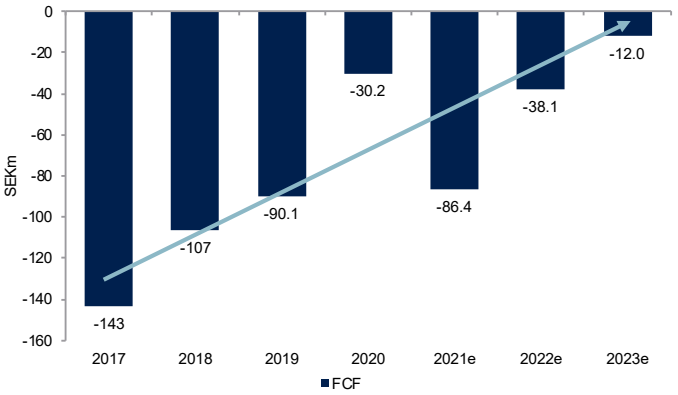


Source: ABG Sundal Collier, company data

We estimate positive EBITDA in 2022

Source: ABG Sundal Collier, company data

Solid improvements in FCF

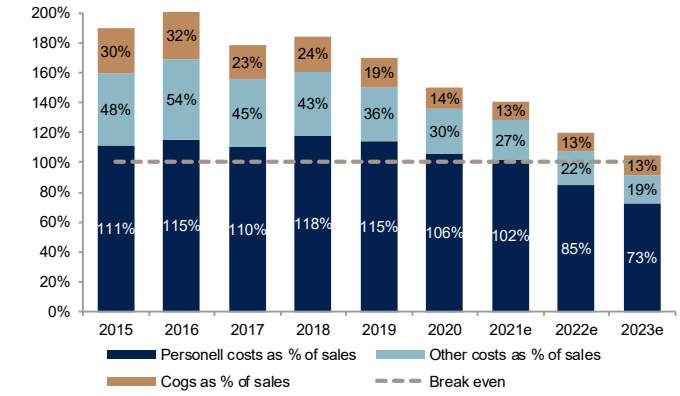


Source: ABG Sundal Collier, company data

A closer look on operating expenses

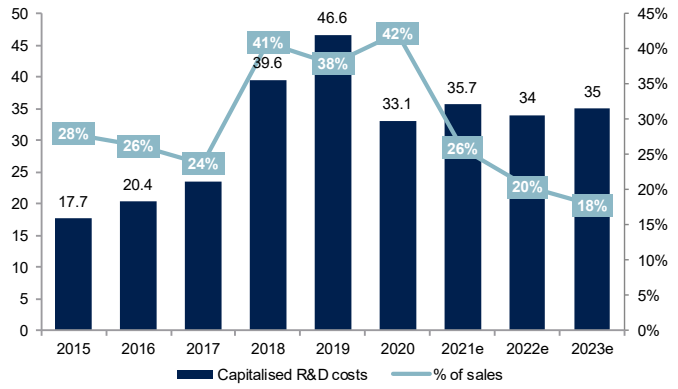
According to the management team, the company has the resources necessary to grow the business, and it does not require significant investments to fuel growth. All cost items have declined as a percentage of sales in recent years, mostly by keeping costs flat and increasing sales. We expect that this development will continue and forecast only small increases in opex items. We estimate net recruitment of two employees p.a. which translates to 3.5% CAGR in personnel costs in '21-'23e. This results in opex growing by 4.5% p.a. vs. sales growth of 18%. We predict that capitalised development (investments in intangible assets) will remain relatively flat around SEK 34-35m per annum in coming years, which translates to ~20% of sales.

Opex breakdown (% of sales)



Source: ABG Sundal Collier, company data

Capitalised development costs to stagnate



Source: ABG Sundal Collier, company data

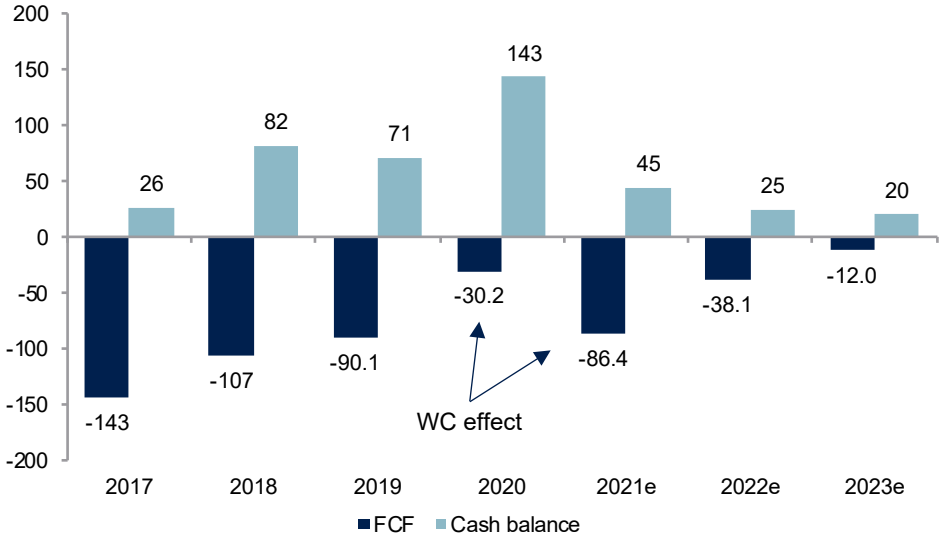
Cash balance and debt

Between 2018 and 2020, Clavister burned through SEK 230m of cash. This was a period, however, where the company was making key strategic transitions while also accelerating development to broaden its portfolio. We estimate that this transitioning has now reached its endpoint. After releasing its SASE solution this fall, the company has successfully broadened its portfolio from one or two main solutions a couple of years ago to six solutions that cater to specific challenges in different industries. Although this is a competitive and R&D-intensive industry, we note that Clavister's international competitors that have reached scale are very profitable, with EBIT margins in the 25-30% range. For Clavister to approach those levels of profitability, it must scale its development costs. We believe that a more mature level of development cost is ~15% of sales vs. ~25% today.

After the share issue in 2020, Clavister currently sits on a cash position of SEK 108m. With the current cash burn, the company will need external financing in the coming years. But if the company managed to reach its growth ambitions while cutting capital expenditures, we think it could manage without external funding until it reaches break-even.

The company also has interest-bearing debt of SEK 223m, most of which is of long-term and comes from financing from the European Investment Bank. We view the fact that Clavister has been granted financing from a European institution to fuel its growth initiatives as a positive, and note that this has contributed with less dilution to shareholders.

Reaching profitability without additional equity financing



Source: ABG Sundal Collier, company data

Breakdown of forecasts

P/L, SEKm	Q1'20	Q2'20	Q3'20	Q4'20	Q1'21	Q2'21	Q3'21e	Q4'21e	2015	2016	2017	2018	2019	2020	2021e	2022e	2023e
Net sales	**29**	**29**	**39**	**31**	**31**	**30**	**42**	**35**	**64**	**78**	**100**	**112**	**123**	**129**	**138**	**167**	**197**
COGS	-5	-5	-4	-4	-4	-5	-4	-4	-19	-25	-23	-26	-24	-18	-18	-22	-26
Gross result	**24**	**24**	**35**	**27**	**26**	**25**	**38**	**31**	**45**	**53**	**77**	**85**	**99**	**111**	**120**	**145**	**171**
Other revenues	4	0	2	6	1	2	1	1	0	0	1	1	0	11	5	5	5
OPEX	-34	-32	-29	-47	-34	-32	-29	-46	-85	-111	-131	-140	-139	-142	-141	-144	-145
Non-recurring items	0	0	0	0	0	0	0	0	0	0	0	0	-10	0	0	0	0
EBITDA	**-6**	**-9**	**9**	**-16**	**-8**	**-6**	**10**	**-14**	**-40**	**-58**	**-54**	**-54**	**-39**	**-19**	**-16**	**6**	**32**
D&A	-12	-9	-8	-8	-9	-9	-8	-8	-12	-15	-23	-36	-48	-37	-34	-31	-31
EBITA	**-8**	**-10**	**7**	**-17**	**-10**	**-7**	**7**	**-16**	**-41**	**-61**	**-57**	**-62**	**-53**	**-28**	**-26**	**-3**	**22**
EBIT	**-17**	**-17**	**1**	**-23**	**-16**	**-14**	**2**	**-22**	**-52**	**-72**	**-77**	**-90**	**-87**	**-56**	**-50**	**-25**	**1**
Net financials	-22	5	-10	3	-10	-5	-4	-4	-4	1	-7	-28	-32	-24	-23	-22	-22
EBT	**-40**	**-12**	**-9**	**-20**	**-26**	**-19**	**-2**	**-26**	**-56**	**-72**	**-84**	**-118**	**-119**	**-81**	**-73**	**-47**	**-21**
Tax	0	0	-1	0	0	0	0	0	13	17	17	-5	-76	0	0	0	0
Net income	**-39**	**-12**	**-10**	**-20**	**-26**	**-19**	**-2**	**-26**	**-43**	**-55**	**-66**	**-123**	**-195**	**-81**	**-73**	**-47**	**-21**
EPS basic (SEK)	**-1.5**	**-0.5**	**-0.4**	**-0.5**	**-0.5**	**-0.3**	**0.0**	**-0.5**	**-2.5**	**-2.7**	**-2.9**	**-5.2**	**-7.6**	**-2.1**	**-1.3**	**-0.9**	**-0.4**
Growth metrics																	
Sales growth q-o-q	-8%	-3%	38%	-22%	-1%	-3%	42%	-16%									
Sales growth y-o-y	9%	-13%	24%	-4%	4%	4%	7%	15%		21%	28%	12%	10%	5%	7%	21%	18%
EBITA growth y-o-y	-26%	8%	-206%	-20%	28%	-29%	7%	-9%		51%	-8%	9%	-14%	-47%	-7%	-87%	-737%
EBIT growth y-o-y	-7%	-4%	-109%	-23%	-8%	-18%	45%	-7%		39%	6%	17%	-3%	-35%	-12%	-49%	-104%
Margins																	
Gross margin	83%	83%	90%	86%	85%	84%	90%	88%	70%	68%	77%	76%	81%	86%	87%	87%	87%
EBITA margin	-27%	-36%	18%	-57%	-34%	-25%	18%	-45%	-63%	-79%	-57%	-55%	-43%	-22%	-19%	-2%	11%
EBIT margin	-59%	-60%	3%	-76%	-52%	-48%	4%	-61%	-81%	-93%	-77%	-81%	-71%	-44%	-36%	-15%	1%
FCF & cash position																	
FCF (lease adj.)	-11	-1	-21	-19	-46	-3			-50	-62	-143	-107	-97	-36	-94	-45	-19
Cash position	69	68	31	143	111	108			44	75	26	82	71	143	45	25	20
R12m FCF	-78	-59	-57	-52	-87	-89											

Source: ABG Sundal Collier, company data

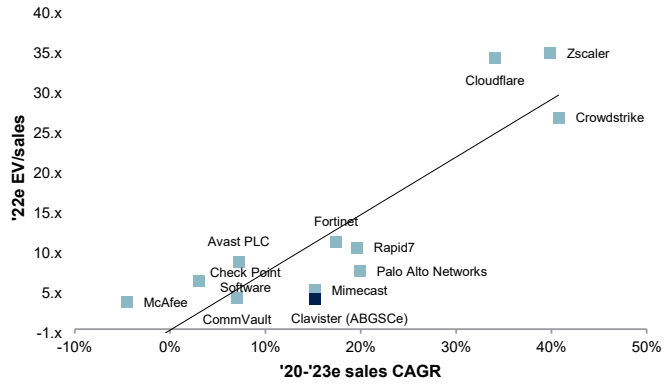
Valuation

To arrive at a fair value range for Clavister, we have looked at peer multiples for international cybersecurity firms, and constructed DCF models using three scenarios. In the peer valuation, we looked at EV/sales and EV/EBITDA multiples and compared them to sales growth. In the DCF, we used a span of growth rates (13% to 20% CAGR) and profitability levels (14% to 17% avg. for '25e-'30e EBIT margin) across our three scenarios. We arrive at a fair value range of SEK 5-16 per share by using a blend of the two methods. This is a wide range, but we believe it is fair until the company has demonstrated the ability to generate positive free cash flow.

Peer valuation

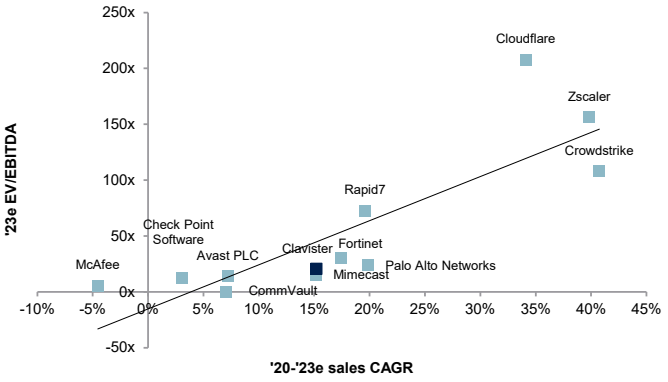
By comparing Clavister with other cybersecurity firms, our assessment is that it could be fairly valued at a range of 4x-7x '22e EV/sales and 20x-30x EV/EBITDA. Based on this, we arrive at a fair value range of SEK 7-20 per share. The range is wide for two reasons: 1) Clavister's high growth and gross margin warrants a high multiple and 2) the low current profitability warrants a lower multiple.

EV/sales vs. sales CAGR



Source: ABG Sundal Collier, company data, FactSet Consensus

EV/EBITDA vs. sales CAGR



Source: ABG Sundal Collier, company data, FactSet Consensus

As we expect that Clavister will reach a positive EBITDA next year, we decided to look at EV/EBITDA multiples for 2025e, where we believe the company will be able to generate more sustainable profitability levels. Below, we see the potential valuation and IRR of different implied 2025e multiples.

Based on '25e EV/EBITDA multiples of 16x-30x, we calculate annualised returns of 14-41%

Financial overview	Actual			ABGSC estimate			Extended		CAGR	
SEKm	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**	**2024e**	**2025e**	**20-'23e**	**20-'25e**
Sales	**112**	**123**	**129**	**138**	**167**	**197**	**226**	**260**	15.2%	15.1%
y-o-y	*12.2%*	*10.1%*	*4.6%*	*7.1%*	*21.0%*	*18.0%*	*15.0%*	*15.0%*		
Gross profit	**85**	**99**	**111**	**121**	**145**	**171**	**206**	**238**	15.6%	16.5%
Gross margin	*76.3%*	*80.5%*	*86.2%*	*87.7%*	*87.0%*	*87.0%*	*91.0%*	*91.5%*		
Capitalised development costs	**40**	**47**	**33**	**36**	**34**	**35**	**36**	**39**	1.9%	3.4%
% of sales	*35.4%*	*37.9%*	*25.7%*	*25.9%*	*20.4%*	*17.8%*	*16.0%*	*15.0%*		
Opex	**-140**	**-139**	**-142**	**-141**	**-144**	**-145**	**-158**	**-176**	0.6%	4.4%
% of sales	*125.5%*	*112.6%*	*110.2%*	*102.2%*	*86.7%*	*73.5%*	*70.0%*	*67.5%*		
EBITDA	**-54**	**-39**	**-19**	**-15**	**6**	**32**	**48**	**62**		
EBITDA margin	*(48.5%)*	*(31.7%)*	*(15.1%)*	*(11.0%)*	*3.3%*	*16.1%*	*21.0%*	*24.0%*		
D&A	**-36**	**-48**	**-37**	**-34**	**-31**	**-31**	**-31**	**-31**		
EBIT	**-90**	**-87**	**-56**	**-49**	**-25**	**1**	**17**	**32**		
EBIT margin	*(80.6%)*	*(70.8%)*	*(43.8%)*	*(35.6%)*	*(15.3%)*	*0.6%*	*7.5%*	*12.3%*		
Valuation scenario										
EV/EBITDA 2025e	**16x**	**18x**	**20x**	**22x**	**24x**	**26x**	**28x**	**30x**		
EV	999	1124	1249	1373	1498	1623	1748	1873		
Net debt incl. cash burn until 2025	350	350	350	350	350	350	350	350		
Market cap	**649**	**774**	**899**	**1023**	**1148**	**1273**	**1398**	**1523**		
Implied share price 2025	**11.0**	**13.1**	**15.2**	**17.3**	**19.4**	**21.5**	**23.6**	**25.7**		
Annualised return	***14%***	***19%***	***23%***	***27%***	***31%***	***34%***	***38%***	***41%***		

Source: ABG Sundal Collier, company data

DCF indicates a fair value range of SEK 3-13 per share

We have constructed a DCF analysis with three different scenarios. The scenarios are quite similar, and mainly differ in terms of expected sales growth and the scale effect this has on the operating margin.

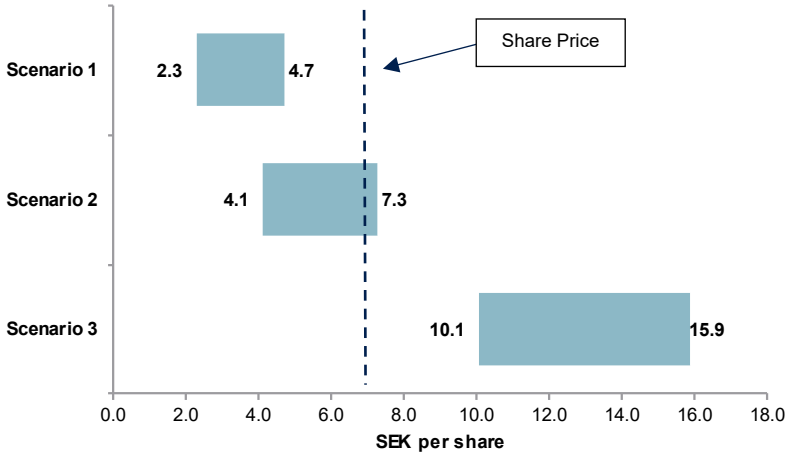
DCF: three scenarios

Scenario 1		Scenario 2		Scenario 3	
Sales CAGR '22e-'30e	**13%**	**Sales CAGR '22e-'30e**	**16%**	**Sales CAGR '22e-'30e**	**20%**
Avg. EBIT margin '25e-'30e	14%	Avg. EBIT margin '25e-'30e	15%	Avg. EBIT margin '25e-'30e	16%
30 EBIT margin	17%	30 EBIT margin	19%	30 EBIT margin	20%
DCF value per share	**3.4**	**DCF value per share**	**5.5**	**DCF value per share**	**12.6**
% of value '21e-'33e	*42%*	*% of value '21e-'33e*	*44%*	*% of value '21e-'33e*	*40%*
Terminal value %	*58%*	*Terminal value %*	*56%*	*Terminal value %*	*60%*
EV/EBITDA '24e	13.9x	EV/EBITDA '24e	13.6x	EV/EBITDA '24e	13.4x
EV/EBITDA '25e	10.3x	EV/EBITDA '25e	9.8x	EV/EBITDA '25e	9.5x
Net debt/EBITDA '24e	4.9x	Net debt/EBITDA '24e	4.8x	Net debt/EBITDA '24e	4.7x

Source: ABG Sundal Collier, company data

By applying +/- 1pp to the WACC in these three scenarios, we arrive at a fair value range for each scenario.

Fair value range DCF, with +/- 1pp to WACC applied



Source: ABG Sundal Collier, company data

Breakdown of the DCF model

Breakdown of DCF scenario 2

DCF model	ABGSC estimates			Extended forecast						
SEKm	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**
Sales	**138**	**167**	**197**	**232**	**274**	**323**	**381**	**439**	**482**	**531**
Sales growth	*7%*	*21%*	*18%*	*18%*	*18%*	*18%*	*18%*	*15%*	*10%*	*10%*
EBITDA	**-15**	**6**	**32**	**49**	**66**	**84**	**103**	**123**	**135**	**154**
EBITDA margin	*-11%*	*3%*	*16%*	*21%*	*24%*	*26%*	*27%*	*28%*	*28%*	*29%*
D&A	-34	-31	-31	-36	-41	-42	-46	-48	-53	-53
EBIT	**-49**	**-25**	**1**	**13**	**25**	**42**	**57**	**75**	**82**	**101**
Cash tax on EBIT	0	0	0	-3	-5	-8	-11	-15	-16	-20
NOPLAT	**-49**	**-25**	**1**	**10**	**20**	**34**	**46**	**60**	**66**	**81**
WC investment	-17	7	8	8	7	8	10	7	7	10
Capex	-36	-34	-35	-39	-44	-45	-48	-48	-53	-53
Free cash flow	**-74**	**-28**	**-2**	**7**	**17**	**31**	**47**	**59**	**66**	**84**

Assumptions	
Growth rate '21-'30	16%
EBIT margin '30	19%
Terminal growth	1.0%
WACC	10.0%

Source: ABG Sundal Collier, company data

Risks

Competition
Most of Clavister's revenue comes from medium-sized or large customers. The importance of these accounts is reflected in the consolidated revenue and strategic decisions. Because Clavister competes with more established, multinational cybersecurity vendors, there is an inherent risk of customers picking a more established vendor with a more well-known brand than Clavister.

Technology
Clavister's operational success is tied to its technology. There is a risk that Clavister could underestimate the development time for programming and testing, which can lead to projects being delayed and customers picking a competitor instead. In addition, the technology can contain errors that could lead to Clavister losing customers and/or finding it more difficult to attract new ones.

Supplier dependence
A part of Clavister's business is dependent on hardware. If suppliers cannot deliver the agreed-upon-volume on time, it could affect deliveries to customers, which can damage customer relationships and result in lower revenue.

Key personnel
As with many other technology firms, Clavister is dependent on key personnel. Managers leaving could therefore influence the business significantly.

Business interruptions
Clavister's operational and financial performance can be impacted by business interruptions, as a result of restrictions imposed by governments around the world.

Intangible assets
Clavister's intangible technology is not currently patented. There is a risk that Clavister utilises technology protected by other firms' intellectual property, which may result in damages or claims. Clavister could also be incorrectly accused of encroaching on other firms' intellectual property, and be dragged into costly patent litigations.

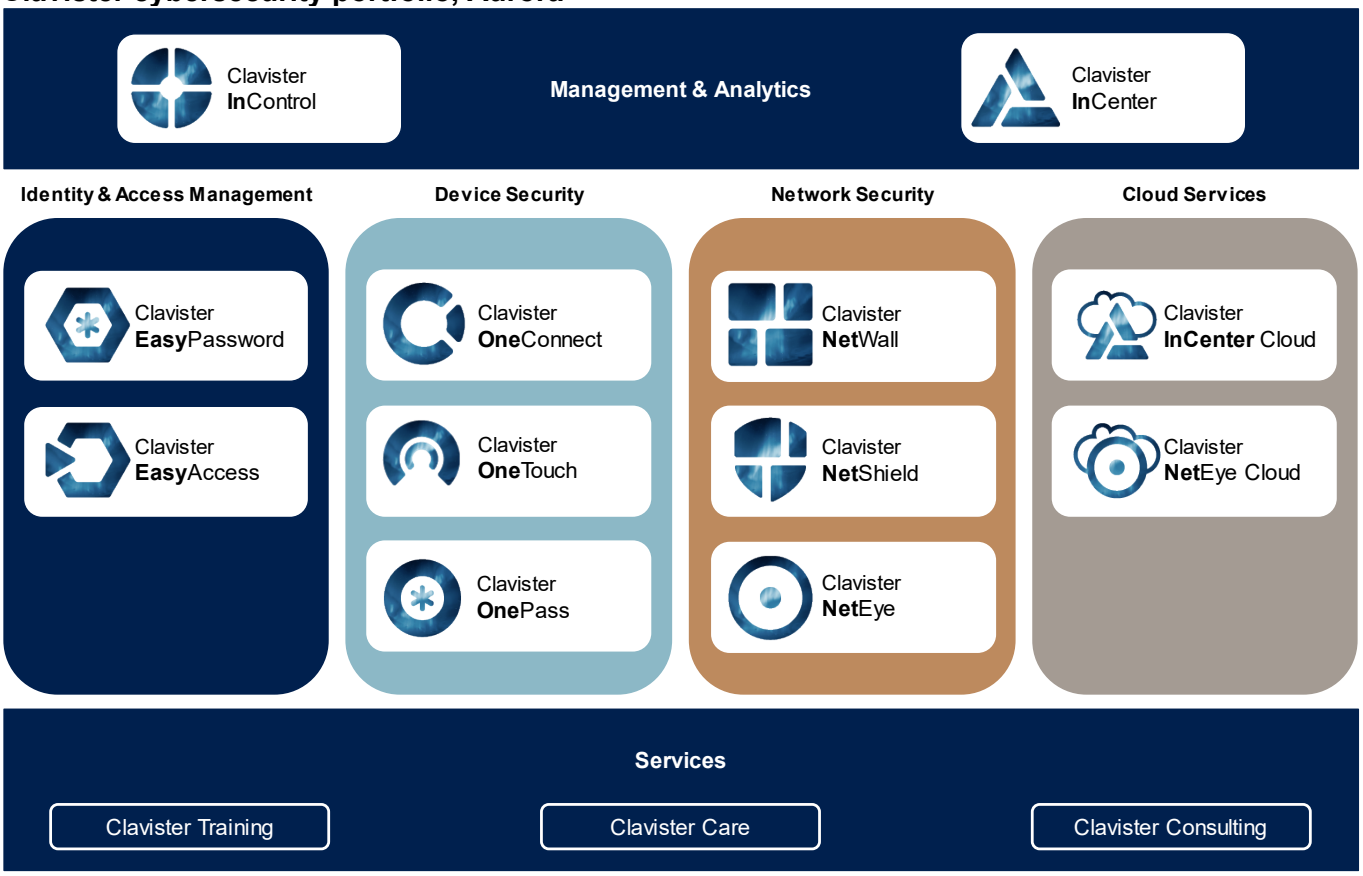
Economic factors
Clients' willingness to buy from Clavister could be affected by economic factors. In an economic downturn, things like network security investment can be put on hold. There is always a risk that agreements made between Clavister and a customer lack sufficient coverage, despite legal expertise and internally-dedicated resources.

Financial risk
Clavister is subject to currency risk. The majority of its sales take place in EUR, SEK and USD. Currency fluctuations applicable to both payments to suppliers and from customers can create currency losses. Clavister hedges its currency risk by offsetting incoming and outgoing payments in equal currency. In 2020, sales in EUR accounted for 47% of group sales, followed by the SEK (46%) and the USD (6%). 75% of opex was nominated in SEK, with the rest split between EUR and USD. Clavister is subject to interest risk through its convertible loan (due 22 March 2022), as well as from factoring.

Appendix I – technology platform

Clavister has invested more than EUR 60m over the last 20 years into its technology platform. This has manifested in 12 cybersecurity products and services spanning five product families, which on aggregate cater to over 40 specific cybersecurity use-cases, from firewall functionality, to cryptography and identification. What sets Clavister's technology platform apart from the competition is its high share of proprietary software. By owning +75% of the software used in the product portfolio, Clavister is well positioned to license its software in a sophisticated way.

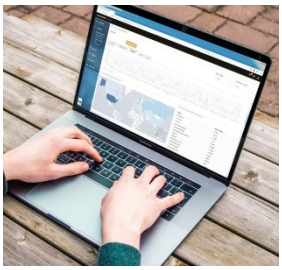
Clavister cybersecurity portfolio, Aurora



Source: ABG Sundal Collier, company data

The Aurora product suite

In 2019, Clavister launched its new Aurora Security Framework. It is a holistic approach to link security siloes. On the platform, products that complement and strengthen each other are bundled together to form complete and modern security solutions. With the launch, it released 10 upgrades to existing or new products. For Clavister, this marked a transition from being a product company that offered a couple of siloes products, to a full portfolio and solution provider. Instead of relying on other suppliers to complement their end customer offering, customers can now rely on Clavister for complete solutions to solve their security challenges, which puts the firm in a better position to expand its footprint with customers. The next chapter goes through Clavister's products, which are combined into six pre-defined solutions that solve specific industry needs.

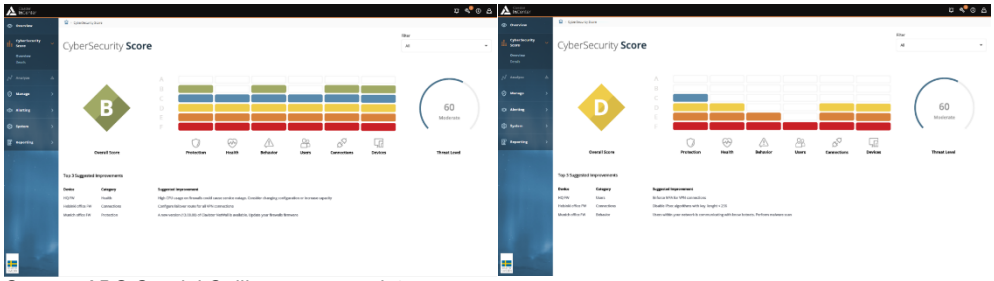


Products/Modules

Clavister InCenter is an analytical tool that enables a good overview of the environment, traffic, and current threats. Almost all implement firewalls. Many do it retroactively. The ability to take real-time action is what is necessary. This is where Clavister InCenter comes into action. It gives IT-managers a holistic view of threats and traffic with the capabilities of detecting anomalies with its easy to use user interface. It will also drive down TCO compared to third-party log management systems. Clavister InCenter serves as the foundation of the Aurora Security Framework, providing holistic management and analytics for all products in the portfolio. It maximises the synergies of all product areas: identity and access management, device security, network security, and cloud services. In addition, it enables businesses to connect their locations with each other and the internet in a secure and reliable way, enables inspection of traffic and behaviour to protect digital assets from threats and preventative security measures that can reduce the risk of users making mistakes that compromises the security of a business.

Included in Clavister InCenter is a CyberSecurity Score that offers simplified, actionable security analytics. As cybersecurity is becoming a business priority, simplicity is key. This solution helps IT managers and their executives to communicate about the status of their security infrastructure and ensure that funds and efforts are spent where they matter the most.

Cybersecurity Score (on the Clavister InCenter platform)



Source: ABG Sundal Collier, company data

Clavister InCenter Cloud enables IT administrators to gain insights into their network security with little setup and no hardware investments. It provides users with forensics with log searches, dashboarding, alerting, reporting and health monitoring.

Clavister InControl is a premium centralised management system, designed to handle thousands of Clavister Next-Generation Firewalls in large networks. Zero-touch positioning support allows newly deployed firewalls to automatically find their way to the right Clavister InControl server. From there, the system enables safe onboarding and policy deployment. With integrated support for reporting, configuration management and version control, Clavister InControl is the ideal centralised management solution for large enterprises and Managed Security Service Providers (e.g. SD-WAN vendors).

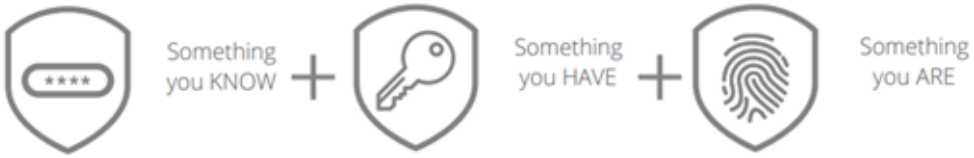
InControl and InCenter functions

Clavister InControl	Clavister InCenter	Clavister InCenter Cloud
▪ **Zero Touch Provisioning** – setup and running in minutes ▪ **Rapid config** with Hub & Spoke VPN Templates ▪ **Shared policies** between multiple firewalls ▪ **Smooth and powerful** firmware upgrade management ▪ **Multi-Tenancy**	▪ Optional Clavister InCenter to run in **private cloud datacenter** ▪ Enables **extended storage** capabilities ▪ Enables single tenant **private instances**	▪ **Security Analytics** with real-time dashboards ▪ **Alerting and Reporting** ▪ **Forensics** with 30 aggregated +3 days raw data ▪ **Multi-Tenant** hosted by Clavister ▪ **CyberSecurity ScoreCard** with prescriptive analytics

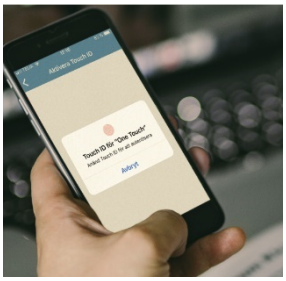
Source: company data

Clavister EasyAccess with Multi Factor Authentication (MFA) provides the security needed to protect a system or environment from one of the major reasons for larger security incidents and breaches: the simple combination of usernames and passwords.

Multi Factor Authentication



Source: company data



Clavister OneTouch is a mobile application used for biometrical authorisation of any multi-factor login request. With OneTouch, there is no need to worry about passwords. Just use a thumb print or face recognition to unlock all the applications and services securely.

With Clavister EasyPassword, there is no need to call the IT administrators to give a new password because the password was lost. With EasyPassword, individuals can create a new password by themselves in no time.

Clavister NetShield is one of Clavister's flagship products. It is a Service-Based Firewall (SBFW), a revolutionary product that caters to the needs of modern network users and is ideal for data centre protection and network infrastructure requiring carrier-grade speeds and features. Besides flexible perimeter protection, the product can terminate secure traffic to a web-server farm and perform inspection with built in intrusion and a detection system both securing and offloading the server infrastructure. Its carrier services and routing functionality makes this product ideal for large network protection such as campus networks, public Wi-Fi or mobile and fixed communication service provider networks. Clavister NetShield can be deployed in a high throughput appliance or deployed virtually, optimised for performance in KVM and VMW environments.

Clavister NetWall represents the Next-Generation Firewall solution. NetWall's compact, fast, and powerful desktop appliances deliver complete security use cases for remote offices or as CPEs. For larger enterprise users or deployments at headquarters, Clavister's rack mountable appliances give best in class protection for even the biggest companies. In addition, Clavister has been a pioneer in virtual products since 2008 and uses a record low amount of resources, which makes it ideal for creating secure cells in cloud environments.

Clavister OneConnect is Clavister's SSL VPN Client that offers a simple and easy to use solution for remote access using the Clavister NetWall Next-Generation Firewalls. Connecting securely is done easily by utilising the built-in provisioning portal in Clavister NetWall. With support for Microsoft Windows and Apple macOS there is support for a wide range of devices. Together with Clavister EasyAccess, OneConnect provides a unique one-click access experience for the user to start with VPN connectivity.

Services

Clavister's customers are offered two types of services: the comprehensive, all-inclusive Clavister Security Subscription (CSS), or the more cost-efficient Clavister Product Subscription (CPS), which can be upgraded to a CSS at any time. Clavister Product Subscription includes both software services, such as upgrades and maintenance and direct vendor support, as well as central management system Clavister InControl. Alternatively, the Clavister Security Subscription (CSS) includes all of the services in the CPS, with the addition of the full Next-Generation Firewall and services like Anti-Virus, Web Content Filtering, Intrusion Detection and Prevention (IDP), IP reputation intelligence and true Application Control.

Appendix II – security use cases

Security use-cases addressed by Clavister's products

Clavister's solutions are supporting users, who need to secure their access or authentication to services. Clavister is securing devices, is a part of physical and radio networks, and exists in sites, in vehicles, and in private datacentres or in the public clouds. The current offering addresses more than 20 different use-cases, in three different categories: 1) To enable customers to connect to networks or internally, 2) to protect their perimeters and assets from threats, and 3) to prevent security breaches.

Security use-cases addressed by Clavister's products

Source: ABG Sundal Collier, company data

Appendix III – senior management

Management team overview

John Vestberg
President & CEO

Position held since 2017

Selected experience:

- Co-founder of Clavister
- CTO until taking over as CEO in 2017
- Prior to co-funding Clavister, John ran an IT consulting firm conducting projects for public administrations and private firms
- Holdings in Clavister: 524,520 shares and 500,000 warrants

Przemek Sienkiewicz
Chief Commercial Officer

Position held since 2017

Selected experience:

- 20 years of operational experience managing established business and start-ups
- Experience from firms like Oracle, Google and IBM
- Holdings in Clavister: 85,777 shares and 250,000 warrants

Nils Undén
Chief Technology Officer

Position held since 2020

Selected experience:

- Experience from engineering management roles at large international product organisations, start-ups across CRM, logistics, fintech and telecom solution providers
- Holdings in Clavister: 37,000 shares and 200,000 warrants

Johan Edlund
Chief Products Officer

Position held since 2018

Selected experience:

- Experience as Commercial Manager Cloud at Aptilo Networks, Managing Director at Procera Networks AB and VP Product Management at Procera Networks Inc.
- Earlier in the career, Johan was VP Product Management at Clavister and had several roles within Telco Group 3
- Holdings in Clavister: 35,800 shares and 250,000 warrants

David Nordström
Chief Financial Officer

Position held since 2020

Selected experience:

- Experience as authorised auditor, having been with PwC in Stockholm since 2011. David has been in chare of larger auditing projects towards publicly listed clients
- Holdings in Clavister: 11,833 shares and 250,000 warrants

Adrianne Edblad
Chief People and Culture Officer

Position held since 2018

Selected experience:

- Several years of experience working with HR in global companies withing IT, services, and mass media industry
- Experience of strategic and tactic HR projects with companies like Thomson Reuters, Point Carbon and Sutherland
- Holdings in Clavister: 2,283 shares and 200,000 warrants

Source: company data

Appendix IV – board of directors

Board of directors

Viktor Kovacs
Chairman of the Board

Elected to the board in 2017

Selected experience:

- Significant experience in go-to-market strategy and execution with growth-stage companies in the ICT sector
- Viktor has held executive roles in EDS Corp. (now HP), Octel Communications (sold to Lucent), Portal Software (now Oracle), Cisco, and others
- Holdings in Clavister: 17,000 shares

Jan Frykhammar
Director

Elected to the board in 2018

Selected experience:

- 26 years of work experience from various roles at Ericsson, being Group CFO from 2009 and subsequently interim CEO of Ericsson Group from July 2016 until January 2017
- Holdings in Clavister: 45,725 shares

Kimberly Matenchuk
Director

Elected to the board in 2019

Selected experience:

- Kimberly is a Managing Director of Ricardo Software
- She has over 10 years' experience in global and digital software sales (including 10 years at Google), developing and executing Go-To-Market strategies, and leading enterprise sales teams across Europe
- Holdings in Clavister: 15,264 shares

Staffan Dahlström
Director

Elected to the board in 2018

Selected experience:

- CEO of HMS Networks AB (listed on Nasdaq OMX Mid CAP) since 2009 and one of its co-founders
- Holdings in Clavister: 964,946 shares

Martin Roos
Director

Elected to the board in 2021

Selected experience:

- Chairman roles in global TMT industry and several CEO roles within the same industry. Now Chairman at Strata Analytics group and non-executive board of director at Rencom, BIMA AB and Seamless Distribution Systems
- Holdings in Clavister: 528,584 shares

Martin Kreuzer
Director

Elected to the board in 2020

Selected experience:

- Fifteen years of experience from intelligence work and information security matters as Civil Servant at German intelligence services – amongst others in counter-economic espionage and counter cyber warfare
- Martin is currently Risk Manager for Cyber Risks in Cyber Insurance at Munich Re
- Holdings in Clavister: 8,500 shares

Malte Pollmann
Director

Elected to the board in 2021

Selected experience:

- Member of the Utimaco Management Board since 2008, and CEO for the company 2011-2019. Currently Chief Strategy Officer at Utimaco
- Serves on the Supervisory Board of the International School of IT Security (ISITS) AG in Bochum
- Holdings in Clavister: No

Source: company data

Appendix V – ownership structure

Ten largest shareholders

#	Shareholder	No. of shares	Holding (%)
1	HSBC Trinkhaus and Burkhart AG, Duesseldorf, WS	6,221,148	11.3%
2	Försäkringsbolaget, Avanza Pension	4,572,842	8.3%
3	Goldman Sachs International LTD, W8IMY	3,395,528	6.2%
4	Nordnet Pensionsförsäkring AB	2,368,904	4.3%
5	AB Stena Finans	1,756,462	3.2%
6	Swedbank Försäkring	1,679,720	3.1%
7	RBC Investor Services Bank S.A	1,466,666	2.7%
8	Danske Bank International S.A	1,197,065	2.2%
9	RGG ADM-Gruppen AB	1,192,961	2.2%
10	Pension, Futur	1,025,183	1.9%
	Ten largest shareholders	**24,876,479**	**45.4%**
	Other shareholders	29,950,092	54.6%
	Total	**54,826,571**	**100.0%**

Source: ABG Sundal Collier, company data
Updated: 30 Aug 2021

Income Statement (SEKm)	Q1 2020	Q2 2020	Q3 2020	Q4 2020	Q1 2021	Q2 2021	Q3 2021e	Q4 2021e
Sales	29	29	39	31	31	30	42	35
COGS	0	0	0	0	0	0	0	0
Gross profit	29	29	39	31	31	30	42	35
Other operating items	-36	-37	-31	-47	-39	-35	-33	-49
EBITDA	**-6**	**-9**	**9**	**-16**	**-8**	**-6**	**10**	**-14**
Depreciation and amortisation	-2	-2	-2	-2	-2	-2	-2	-2
EBITA	**-8**	**-10**	**7**	**-17**	**-10**	**-7**	**7**	**-16**
EO items	0	0	0	0	0	0	0	0
Impairment and PPA amortisation	-9	-7	-6	-6	-6	-7	-6	-6
EBIT	**-17**	**-17**	**1**	**-23**	**-16**	**-14**	**2**	**-22**
Net financial items	-22	5	-10	3	-10	-5	-4	-4
Pretax profit	**-40**	**-12**	**-9**	**-20**	**-26**	**-19**	**-2**	**-26**
Tax	0	0	-1	-0	0	-0	0	0
Net profit	**-39**	**-12**	**-10**	**-20**	**-26**	**-19**	**-2**	**-26**
Minority interest	0	0	0	0	0	0	0	0
Net profit discontinued	0	0	0	0	0	0	0	0
Net profit to shareholders	**-39**	**-12**	**-10**	**-20**	**-26**	**-19**	**-2**	**-26**
EPS	-1.54	-0.48	-0.39	-0.52	-0.49	-0.35	-0.04	-0.47
EPS Adj	-1.18	-0.21	-0.17	-0.37	-0.38	-0.22	0.06	-0.36
Total extraordinary items after tax	0	0	0	0	0	0	0	0
Tax rate (%)	*0.0*	*0.3*	*9.2*	*0.4*	*0.4*	*0.1*	*0*	*0*
Gross margin (%)	*100.0*	*100.0*	*100.0*	*100.0*	*100.0*	*100.0*	*100.0*	*100.0*
EBITDA margin (%)	*-21.5*	*-30.6*	*21.7*	*-51.2*	*-26.3*	*-19.9*	*22.6*	*-38.2*
EBITA margin (%)	*-27.3*	*-36.2*	*17.6*	*-56.7*	*-33.5*	*-25.0*	*17.6*	*-44.7*
EBIT margin (%)	*-59.0*	*-60.0*	*3.2*	*-75.5*	*-52.2*	*-47.7*	*4.3*	*-60.8*
Pretax margin (%)	*-134.7*	*-43.1*	*-23.2*	*-64.9*	*-86.3*	*-64.1*	*-5.2*	*-72.1*
Net margin (%)	*-134.6*	*-42.9*	*-25.3*	*-65.2*	*-86.0*	*-64.1*	*-5.2*	*-72.1*
Growth rates Y/Y	**Q1 2020**	**Q2 2020**	**Q3 2020**	**Q4 2020**	**Q1 2021**	**Q2 2021**	**Q3 2021e**	**Q4 2021e**
Sales growth (%)	*9.0*	*-12.7*	*23.7*	*-3.6*	*4.3*	*3.6*	*7.0*	*15.0*
EBITDA growth (%)	*+chg*	*-chg*	*+chg*	*+chg*	*-chg*	*+chg*	*11.6*	*+chg*
EBIT growth (%)	*+chg*	*+chg*	*+chg*	*+chg*	*+chg*	*+chg*	*45.1*	*+chg*
Net profit growth (%)	*-chg*	*+chg*	*+chg*	*+chg*	*+chg*	*-chg*	*+chg*	*-chg*
EPS growth (%)	*-chg*	*+chg*	*+chg*	*+chg*	*+chg*	*-chg*	*+chg*	*-chg*
Adj earnings numbers	**Q1 2020**	**Q2 2020**	**Q3 2020**	**Q4 2020**	**Q1 2021**	**Q2 2021**	**Q3 2021e**	**Q4 2021e**
EBITDA Adj	-6	-9	9	-16	-8	-6	10	-14
EBITDA Adj margin (%)	*-21.5*	*-30.6*	*21.7*	*-51.2*	*-26.3*	*-19.9*	*22.6*	*-38.2*
EBITA Adj	-8	-10	7	-17	-10	-7	7	-16
EBITA Adj margin (%)	*-27.3*	*-36.2*	*17.6*	*-56.7*	*-33.5*	*-25.0*	*17.6*	*-44.7*
EBIT Adj	-17	-17	1	-23	-16	-14	2	-22
EBIT Adj margin (%)	*-59.0*	*-60.0*	*3.2*	*-75.5*	*-52.2*	*-47.7*	*4.3*	*-60.8*
Pretax profit Adj	-30	-5	-3	-14	-21	-12	3	-20
Net profit Adj	-30	-5	-4	-14	-21	-12	3	-20
Net profit to shareholders Adj	-30	-5	-4	-14	-21	-12	3	-20
Net Adj margin (%)	*-103.0*	*-19.2*	*-10.9*	*-46.4*	*-67.3*	*-41.5*	*8.1*	*-56.0*

Source: ABG Sundal Collier, Company data

Income Statement (SEKm)	na	2015	2016	2017	2018	2019	2020	2021e	2022e	2023e
Sales	na	64	78	100	112	123	129	138	167	197
COGS	na	-19	-25	-23	-26	-24	-18	-18	-22	-26
Gross profit	na	45	53	77	85	99	111	120	145	171
Other operating items	na	-85	-111	-131	-140	-138	-130	-136	-139	-140
EBITDA	**na**	**-40**	**-58**	**-54**	**-54**	**-39**	**-19**	**-16**	**6**	**32**
Depreciation and amortisation	na	-1	-1	-2	-1	-8	-9	-8	-9	-10
Of which leasing depreciation	na	0	0	0	0	-7	-7	-7	-7	-8
EBITA	**na**	**-41**	**-61**	**-57**	**-62**	**-53**	**-28**	**-26**	**-3**	**22**
EO items	na	0	0	0	0	-10	0	0	0	0
Impairment and PPA amortisation	na	-12	-11	-20	-28	-34	-28	-24	-22	-21
EBIT	**na**	**-52**	**-72**	**-77**	**-90**	**-87**	**-56**	**-50**	**-25**	**1**
Net financial items	na	-4	1	-7	-28	-32	-24	-23	-22	-22
Pretax profit	**na**	**-56**	**-72**	**-84**	**-118**	**-119**	**-81**	**-73**	**-47**	**-21**
Tax	na	13	17	17	-5	-76	-0	0	0	0
Net profit	**na**	**-43**	**-55**	**-66**	**-123**	**-195**	**-81**	**-73**	**-47**	**-21**
Minority interest	na	0	0	0	0	0	0	0	0	0
Net profit discontinued	na	0	0	0	0	0	0	0	0	0
Net profit to shareholders	**na**	**-43**	**-55**	**-66**	**-123**	**-195**	**-81**	**-73**	**-47**	**-21**
EPS	na	0	0	-11.43	-5.22	-7.59	-2.08	-1.33	-0.87	-0.38
EPS Adj	*na*	*0*	*0*	*-11.43*	*-5.22*	*-7.19*	*-2.08*	*-1.33*	*-0.87*	*-0.38*
Total extraordinary items after tax	na	0	0	0	0	-10	0	0	0	0
Leasing payments	na	0	0	0	0	-7	-7	-7	-7	-8
Tax rate (%)	*na*	*23.3*	*23.0*	*20.6*	*4.0*	*63.5*	*0.5*	*0.1*	*0*	*0*
Gross margin (%)	*na*	*69.7*	*68.3*	*77.2*	*76.3*	*80.5*	*86.2*	*87.2*	*87.0*	*87.0*
EBITDA margin (%)	*na*	*-62.0*	*-74.2*	*-53.9*	*-48.5*	*-31.7*	*-15.1*	*-11.5*	*3.3*	*16.1*
EBITA margin (%)	*na*	*-63.1*	*-78.9*	*-56.9*	*-55.3*	*-43.4*	*-21.9*	*-18.9*	*-2.1*	*11.2*
EBIT margin (%)	*na*	*-81.1*	*-93.1*	*-77.2*	*-80.6*	*-70.8*	*-43.8*	*-36.1*	*-15.3*	*0.6*
Pretax margin (%)	*na*	*-86.7*	*-92.1*	*-84.0*	*-105.8*	*-96.9*	*-62.9*	*-53.1*	*-28.5*	*-10.6*
Net margin (%)	*na*	*-66.5*	*-70.9*	*-66.7*	*-110.0*	*-158.3*	*-63.1*	*-53.0*	*-28.5*	*-10.6*
Growth rates Y/Y	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
Sales growth (%)	*na*	*na*	*21.2*	*28.0*	*12.2*	*10.1*	*4.6*	*7.1*	*21.0*	*18.0*
EBITDA growth (%)	*na*	*na*	*-45.2*	*7.1*	*-1.0*	*28.0*	*50.2*	*18.5*	*134.9*	*471.6*
EBIT growth (%)	*na*	*na*	*-39.3*	*-6.1*	*-17.2*	*3.3*	*35.3*	*11.7*	*48.8*	*104.3*
Net profit growth (%)	*na*	*na*	*-29.2*	*-20.3*	*-85.2*	*-58.5*	*58.3*	*10.1*	*35.0*	*56.0*
EPS growth (%)	*na*	*na*	*na*	*high*	*54.4*	*-45.6*	*72.6*	*36.1*	*35.0*	*56.0*
Profitability	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
ROE (%)	*na*	*na*	*-36.9*	*-31.8*	*-88.9*	*1,728.6*	*210.4*	*298.8*	*56.1*	*17.6*
ROE Adj (%)	*na*	*na*	*-29.4*	*-22.1*	*-68.4*	*1,337.2*	*137.2*	*201.8*	*30.1*	*-0.1*
ROCE (%)	*na*	*na*	*-41.8*	*-30.6*	*-31.6*	*-33.5*	*-24.6*	*-24.1*	*-15.8*	*0.7*
ROCE Adj(%)	*na*	*na*	*-35.4*	*-22.5*	*-21.6*	*-16.5*	*-12.3*	*-12.6*	*-2.2*	*14.5*
ROIC (%)	*na*	*na*	*-96.3*	*-47.3*	*-61.0*	*-97.5*	*-46.2*	*-43.8*	*-20.0*	*0.8*
ROIC Adj (%)	*na*	*na*	*-96.3*	*-47.3*	*-61.0*	*-85.9*	*-46.2*	*-43.8*	*-20.0*	*0.8*
Adj earnings numbers	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
EBITDA Adj	na	-40	-58	-54	-54	-29	-19	-16	6	32
EBITDA Adj margin (%)	*na*	*-62.0*	*-74.2*	*-53.9*	*-48.5*	*-23.3*	*-15.1*	*-11.5*	*3.3*	*16.1*
EBITDA lease Adj	na	-40	-58	-54	-54	-35	-26	-23	-1	24
EBITDA lease Adj margin (%)	*na*	*-62.0*	*-74.2*	*-53.9*	*-48.5*	*-28.7*	*-20.2*	*-16.7*	*-0.9*	*12.3*
EBITA Adj	na	-41	-61	-57	-62	-43	-28	-26	-3	22
EBITA Adj margin (%)	*na*	*-63.1*	*-78.9*	*-56.9*	*-55.3*	*-35.0*	*-21.9*	*-18.9*	*-2.1*	*11.2*
EBIT Adj	na	-52	-72	-77	-90	-77	-56	-50	-25	1
EBIT Adj margin (%)	*na*	*-81.1*	*-93.1*	*-77.2*	*-80.6*	*-62.4*	*-43.8*	*-36.1*	*-15.3*	*0.6*
Pretax profit Adj	na	-44	-61	-63	-90	-75	-53	-49	-25	0
Net profit Adj	na	-31	-44	-46	-95	-151	-53	-49	-25	0
Net profit to shareholders Adj	na	-31	-44	-46	-95	-151	-53	-49	-25	0
Net Adj margin (%)	na	-48.6	-56.6	-46.4	-84.7	-122.5	-41.2	-35.8	-15.3	0.1

Source: ABG Sundal Collier, Company data

Cash Flow Statement (SEKm)	na	2015	2016	2017	2018	2019	2020	2021e	2022e	2023e
EBITDA	na	-40	-58	-54	-54	-39	-19	-16	6	32
Net financial items	na	-4	1	-7	-28	-32	-24	-23	-22	-22
Paid tax	na	-0	3	-1	-2	-0	0	0	0	0
Non-cash items	na	5	7	1	-24	22	27	5	5	5
Cash flow before change in WC	na	-39	-47	-60	-108	-49	-16	-34	-11	15
Change in WC	na	7	-6	-17	40	-8	40	-17	7	8
Operating cash flow	**na**	**-32**	**-52**	**-77**	**-69**	**-58**	**24**	**-51**	**-4**	**23**
CAPEX tangible fixed assets	na	-0	-0	-2	-2	0	0	0	0	0
CAPEX intangible fixed assets	na	-18	-20	-24	-46	-47	-54	-36	-34	-35
Acquisitions and disposals	na	0	11	0	0	-0	0	0	0	0
Free cash flow	**na**	**-50**	**-62**	**-103**	**-117**	**-105**	**-30**	**-86**	**-38**	**-12**
Dividend paid	na	0	0	0	0	0	0	0	0	0
Share issues and buybacks	na	92	66	13	0	34	185	0	0	0
Lease liability amortisation	na	0	0	0	0	-7	-6	-7	-7	-8
Other non cash items	na	16	43	29	-13	-77	-27	-5	-5	-5
Balance Sheet (SEKm)	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
Goodwill	na	4	54	53	53	52	52	52	52	52
Other intangible assets	na	34	54	97	124	95	120	129	139	151
Tangible fixed assets	na	2	1	2	0	0	0	0	0	0
Right-of-use asset	na	0	0	0	0	20	16	16	16	16
Total other fixed assets	na	49	66	82	77	0	0	0	0	0
Fixed assets	na	90	175	234	254	168	187	196	206	218
Inventories	na	6	7	8	5	8	7	8	8	10
Receivables	na	6	21	34	44	56	45	45	53	61
Other current assets	na	0	0	0	0	0	0	0	0	0
Cash and liquid assets	na	44	75	26	82	71	143	45	25	20
Total assets	**na**	**145**	**277**	**302**	**386**	**303**	**383**	**294**	**292**	**309**
Shareholders equity	na	91	208	210	67	-89	12	-61	-108	-129
Minority	na	0	0	0	0	0	0	0	0	0
Total equity	**na**	**91**	**208**	**210**	**67**	**-89**	**12**	**-61**	**-108**	**-129**
Long-term debt	na	9	8	49	224	220	205	205	235	255
Pension debt	na	0	0	0	0	0	0	0	0	0
Convertible debt	na	9	9	8	8	9	9	9	9	9
Leasing liability	na	0	0	0	0	22	17	17	17	17
Total other long-term liabilities	na	0	3	2	1	1	1	1	1	1
Short-term debt	na	1	11	0	6	54	0	0	0	0
Accounts payable	na	7	12	7	10	5	18	10	12	14
Other current liabilities	na	27	26	27	70	82	121	113	127	143
Total liabilities and equity	**na**	**145**	**277**	**302**	**386**	**303**	**383**	**294**	**292**	**309**
Net IB debt	na	-74	-113	-52	79	233	88	186	237	261
Net IB debt excl. pension debt	na	-74	-113	-52	79	233	88	186	237	261
Net IB debt excl. leasing	na	-24	-47	30	156	212	70	169	219	244
Capital invested	na	17	99	160	147	145	101	126	129	132
Working capital	na	-23	-10	8	-30	-23	-87	-70	-77	-86
EV breakdown	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
Market cap. diluted (m)	na	na	906	527	339	403	271	379	379	379
Net IB debt Adj	na	-24	-47	30	156	234	88	186	237	261
Market value of minority	na	0	0	0	0	0	0	0	0	0
Reversal of shares and participations	na	0	0	0	0	0	0	0	0	0
Reversal of conv. debt assumed equity	na	0	0	0	0	0	0	0	0	0
EV	**na**	**na**	**860**	**557**	**495**	**637**	**358**	**566**	**616**	**640**
Capital efficiency	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
Total assets turnover (%)	*na*	*na*	*36.9*	*34.4*	*32.5*	*35.7*	*37.5*	*40.7*	*56.9*	*65.4*
Working capital/sales (%)	*na*	*na*	*-21.3*	*-1.1*	*-9.8*	*-21.3*	*-42.5*	*-56.9*	*-44.2*	*-41.5*
Financial risk and debt service	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
Net debt/equity	*na*	*-0.81*	*-0.54*	*-0.25*	*1.19*	*-2.61*	*7.29*	*-3.06*	*-2.18*	*-2.02*
Net debt/market cap	*na*	*na*	*-0.12*	*-0.07*	*0.21*	*0.58*	*0.20*	*0.49*	*0.62*	*0.69*
Equity ratio (%)	*na*	*62.8*	*75.2*	*69.4*	*17.3*	*-29.4*	*3.2*	*-20.7*	*-37.1*	*-41.8*
Net IB debt adj./equity	*na*	*-0.27*	*-0.22*	*0.14*	*2.34*	*-2.62*	*7.29*	*-3.06*	*-2.18*	*-2.02*
Current ratio	*na*	*1.54*	*2.11*	*1.98*	*1.54*	*0.92*	*1.35*	*0.76*	*0.59*	*0.56*
EBITDA/net interest	*na*	*-11.04*	*-72.58*	*-7.97*	*-1.93*	*-1.22*	*-0.79*	*-0.68*	*0.25*	*1.44*
Net IB debt/EBITDA	*na*	*1.85*	*1.95*	*0.97*	*-1.46*	*-5.98*	*-4.53*	*-11.77*	*42.79*	*8.26*
Net IB debt/EBITDA lease Adj	*na*	*0.61*	*0.81*	*-0.56*	*-2.88*	*-5.99*	*-2.71*	*-7.36*	*-148.82*	*10.10*
Interest cover	*na*	*-11.24*	*77.10*	*-8.42*	*-2.20*	*-1.67*	*-1.15*	*-1.12*	*-0.16*	*1.00*

Source: ABG Sundal Collier, Company data

Valuation and Ratios (SEKm)	na	2015	2016	2017	2018	2019	2020	2021e	2022e	2023e
Shares outstanding adj.	na	17	21	23	24	26	39	55	55	55
Fully diluted shares Adj	na	17	21	23	24	26	39	55	55	55
EPS	na	0	0	-11.43	-5.22	-7.59	-2.08	-1.33	-0.87	-0.38
Dividend per share Adj	na	0	0	0	0	0	0	0	0	0
EPS Adj	na	0	0	-11.43	-5.22	-7.19	-2.08	-1.33	-0.87	-0.38
BVPS	na	5.22	10.09	9.06	2.83	-3.48	0.31	-1.11	-1.98	-2.36
BVPS Adj	na	3.01	4.87	2.58	-4.68	-9.21	-4.10	-4.41	-5.45	-6.05
Net IB debt / share	na	-4.2	-5.5	-2.2	3.4	9.1	2.3	3.4	4.3	4.8
Share price	na	na	43.90	22.76	14.40	15.71	6.94	6.92	6.92	6.92
Market cap. (m)	na	na	906	527	339	403	271	379	379	379
Valuation	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
P/E	na	na	nm	-2.0	-2.8	-2.1	-3.3	-5.2	-8.0	-18.2
EV/sales	na	na	11.05	5.59	4.43	5.18	2.79	4.11	3.70	3.26
EV/EBITDA	na	na	-14.9	-10.4	-9.1	-16.3	-18.4	-35.7	111.4	20.3
EV/EBITA	na	na	-14.0	-9.8	-8.0	-11.9	-12.7	-21.7	-177.4	29.0
EV/EBIT	na	na	-11.9	-7.2	-5.5	-7.3	-6.4	-11.4	-24.2	581.6
Dividend yield (%)	*na*	*na*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
FCF yield (%)	*na*	*na*	*0*	*-77.6*	*-34.4*	*-25.9*	*-11.1*	*-22.8*	*-10.0*	*-3.2*
Lease adj. FCF yield (%)	*na*	*na*	*nm*	*-77.6*	*-34.4*	*-27.7*	*-13.5*	*-24.7*	*-11.9*	*-5.1*
P/BVPS	na	na	4.35	2.51	5.08	-4.52	22.42	-6.23	-3.50	-2.93
P/BVPS Adj	na	na	9.02	8.83	-3.08	-1.71	-1.69	-1.57	-1.27	-1.14
P/E Adj	na	na	nm	-2.0	-2.8	-2.2	-3.3	-5.2	-8.0	-18.2
EV/EBITDA Adj	na	na	-14.9	-10.4	-9.1	-22.2	-18.4	-35.7	111.4	20.3
EV/EBITA Adj	na	na	-14.0	-9.8	-8.0	-14.8	-12.7	-21.7	-177.4	29.0
EV/EBIT Adj	na	na	-11.9	-7.2	-5.5	-8.3	-6.4	-11.4	-24.2	581.6
EV/cap. employed	na	na	3.6	2.1	1.6	3.0	1.5	3.3	4.0	4.2
Investment ratios	**na**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021e**	**2022e**	**2023e**
Capex/sales	na	27.9	26.3	25.3	42.9	37.9	42.2	25.9	20.4	17.8
Capex/depreciation	na	2,532.1	2,235.0	1,296.3	3,352.4	4,583.4	2,551.8	3,567.2	1,700.0	1,750.0
Capex tangibles/tangible fixed assets	na	0.1	4.5	94.6	1,923.1	nm	nm	nm	nm	nm
Capex intangibles/definite intangibles	na	52.5	37.6	24.2	36.8	49.0	45.3	27.7	24.5	23.2
Depreciation on intangibles/definite inta	na	0.0	0.6	1.1	0.9	1.1	1.8	0.8	1.4	1.3
Depreciation on tangibles/tangibles	na	44.9	63.4	53.2	315.4	nm	nm	nm	nm	nm

Source: ABG Sundal Collier, Company data

Analyst certification

I/We, Simon Granath, Simon Jönsson, the author(s) of this report, certify that not withstanding the existence of any such potential conflicts of interests referred to below, the views expressed in this report accurately reflect my/our personal view about the companies and securities covered in this report.

Analyst valuation methods

ABG Sundal Collier analysts may publish valuation ranges for stocks covered under Company Sponsored Research. These valuation ranges rely on various valuation methods. One of the most frequently used methods is the valuation of a company by calculation of that company's discounted cash flow (DCF). Another valuation method is the analysis of a company's return on capital employed relative to its cost of capital. Finally, the analysts may analyse various valuation multiples (e.g. the P/E multiples and the EV/EBITDA multiples) relative to global industry peers. In special cases, particularly for property companies and investment companies, the ratio of price to net asset value is considered. Valuation ranges may be changed when earnings and cash flow forecasts are changed. They may also be changed when the underlying value of a company's assets changes (in the cases of investment companies, property companies or insurance companies) or when factors impacting the required rate of return change.

Important Company Specific Disclosure

The following disclosures relate to the relationship between ABG Sundal Collier and its affiliates and the companies covered by ABG Sundal Collier referred to in this research report.

Unless disclosed in this section, ABG Sundal Collier has no required regulatory disclosures to make in relation to an ownership position for the analyst(s) and members of the analyst's household, ownership by ABG Sundal Collier, ownership in ABG Sundal Collier by the company(ies) to whom the report(s) refer(s) to, market making, managed or co-managed public offerings, compensation for provision of certain services, directorship of the analyst, or a member of the analyst's household, or in relation to any contractual obligations to the issuance of this research report.

ABG Sundal Collier has undertaken a contractual obligation to issue this report and receives predetermined compensation from the company covered in this report. A redacted version of this research report has been sent to Clavister for the purposes of checking its factual content only. Any changes made have been based on factual input received.

ABG Sundal Collier is not aware of any other actual, material conflicts of interest of the analyst or ABG Sundal Collier of which the analyst knows or has reason to know at the time of the publication of this report.

Production of report: 10/09/2021 06:49 CET.

All prices are as of market close on 08 September, 2021 unless otherwise noted.

Disclaimer

This document has been prepared by ABG Sundal Collier which is the marketing name referring to all or any of ABG Sundal Collier ASA, ABG Sundal Collier AB or ABG Sundal Collier Partners LLP and any of their affiliated or associated companies and their directors, officers, representatives and employees.

This research product is commissioned and paid for by the company covered in this report. As such, this report is deemed to constitute an acceptable minor non-monetary benefit (i.e. not investment research) as defined in MiFID II.

This research product has not been prepared in accordance with legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination.

This report is provided solely for the information and use of investors who are able to make their own investment decisions without undue reliance on this report. The information contained herein does not apply to, and should not be relied upon by, investors with no or limited experience and knowledge from investments in financial instruments. This report is for distribution only under such circumstances as may be permitted by applicable law. Research reports prepared by ABG Sundal Collier are for information purposes only. ABG Sundal Collier accepts no liability whatsoever for any losses arising from any use of this report or its contents. This report is not to be used or considered as an offer to sell, or a solicitation of an offer to buy. The information herein has been obtained from, and any opinions herein are based upon, sources believed reliable, but ABG Sundal Collier makes no representation as to its accuracy or completeness and it should not be relied upon as such. All opinions and estimates herein reflect the judgment of ABG Sundal Collier on the date of this report and are subject to change without notice. Past performance is not indicative of future results.

This research report does not, and does not attempt to contain everything material that there is to be said about Clavister.

The compensation of our research analysts is determined exclusively by research management and senior management, but not including investment banking management. Compensation is not based on specific investment banking revenues, however, it is determined from the profitability of the ABG Sundal Collier Group, which includes earnings from investment banking operations and other business. Investors should assume that ABG Sundal Collier is seeking or will seek investment banking or other business relationships with the companies in this report. The research analyst(s) responsible for the preparation of this report may interact with trading desk and sales personnel and other departments for the purpose of gathering, synthesizing and interpreting market information. From time to time, ABG Sundal Collier and its affiliates and any shareholders, directors, officers or employees thereof may (I) have a position in, or otherwise be interested in, any securities directly or indirectly connected to the subject of this report, or (II) perform investment banking or other services for, or solicit investment banking or other services from, a company mentioned in this report. ABG Sundal Collier relies on information barriers to control the flow of information contained in one or more areas of ABG Sundal Collier, into other areas, units, groups or affiliates of ABG Sundal Collier.

Norway: ABG Sundal Collier ASA is regulated by the Financial Supervisory Authority of Norway (Finanstilsynet); Sweden: ABG Sundal Collier AB is regulated by the Swedish Financial Supervisory Authority (Finansinspektionen); UK: This report is a communication made, or approved for communication in the UK, by ABG Sundal Collier Partners LLP, authorised and regulated by the Financial Conduct Authority in the conduct of its business. US: This report is being distributed in the United States in accordance with FINRA Rule 1050(f)(3)(B) by ABG Sundal Collier Inc., a FINRA member which accepts responsibility for its content. Research analysts are not registered/qualified as research analysts with FINRA or the NYSE, and are not associated persons of ABG Sundal Collier Inc. and therefore not subject to FINRA Rule 2241, the research analyst conflict rules. Research reports distributed in the U.S are intended solely for “major institutional investors”, as defined under Rule 15a-6 of the Securities Exchange Act of 1934. Each U.S major institutional investor that receives a copy of this research report by its acceptance represents that it agrees

it will not distribute this research report to any other person. Any U.S. major institutional investor receiving this report who wishes to effect transactions in any securities referred to herein should contact ABG Sundal Collier Inc., not its affiliates. Further information on the securities referred to herein may be obtained from ABG Sundal Collier Inc., on request.

Singapore: This report is distributed in Singapore by ABG Sundal Collier Pte Ltd, which is not licensed under the Financial Advisers Act (Chapter 110 of Singapore). In Singapore, this report may only be distributed to institutional investors as defined in Section 4A(1)(c) of the Securities and Futures Act (Chapter 289 of Singapore) ("SFA"), and should not be circulated to any other person in Singapore.

This report may not be reproduced, distributed or published by any recipient for any purpose whatsoever without the prior written express permission of ABG Sundal Collier.

Additional information available upon request. If reference is made in this report to other companies and ABG Sundal Collier provides research coverage for those companies details regarding disclosures may be found on our website www.abgsc.com.

.

Norway
Pb. 1444 Vika
NO-0115 OSLO
Norway
Tel: +47 22 01 60 00
Fax: +47 22 01 60 60

Sweden
Regeringsgatan 25, 8th floor
SE-111 53 STOCKHOLM
Sweden
Tel: +46 8 566 286 00
Fax: +46 8 566 286 01

Denmark
Forbindelsesvej 12,
DK-2100 COPENHAGEN
Denmark
Tel: +45 35 46 61 00
Fax: +45 35 46 61 10

United Kingdom
10 Paternoster Row, 5th fl
LONDON EC4M 7EJ
UK
Tel: +44 20 7905 5600
Fax: +44 20 7905 5601

USA
850 Third Avenue, Suite 9-C
NEW YORK, NY 10022
USA
Tel. +1 212 605 3800
Fax. +1 212 605 3801

Germany
Schillerstrasse 2, 5. OG
DE-60313 FRANKFURT
Germany
Tel +49 69 96 86 96 0
Fax +49 69 96 86 96 99

Singapore
10 Collyer Quay
Ocean Financial Center
#40-07, Singapore 049315
Tel +65 6808 6082