CLAVISTER GETS COMPETITIVE BREAK WITH 'SNOWDEN EFFECT,' SEIZES NEW MARKET OPPORTUNITIES

IMPACT REPORT

ANALYSTS

- Brian Partridge
- Adrian Sanabria

NOV 2014

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such. 451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

New York
20 West 37th Street, 6th Floor
New York, NY 10018
Phone: 212.505.3030
Fax: 212.505.2630

London
Paxton House (5th floor), 30 Artillery Lane
London, E1 7LS, UK
Phone: +44 (0) 207 426 0219
Fax: +44 (0) 207 426 4698

San Francisco
140 Geary Street, 9th Floor
San Francisco, CA 94108
Phone: 415.989.1555
Fax: 415.989.1558

Boston
125 Broad Street, 4th Floor
Boston, MA 02109
Phone: 617.275.8818
Fax: 617.261.0688

As the sheer number of personal computing devices, 'things' attaching to the Internet and cloud services explodes, so does the corresponding exposure to security and data integrity risks. IP network security deployed in carriers, cloud providers and at the enterprise edge typically represents a first line of defense that balances the upside of an increasingly connected world with the downside that cyber attacks and breaches can have on business reputations and operations. Network security is one of the oldest market segments in the security space; as a result, it is largely dominated by large vendors, but there are some innovative small players worth paying attention to. Clavister has seen a recent uptick in its opportunities to sell its suite of security appliances and software, notably in the telecom sector. What makes the Clavister story particularly interesting is the direct impact the Snowden revelations have had on the Swedish network security company.

THE 451 TAKE

Clavister has clear challenges and many things going for it as it works its way into more stable financial footing. While growth has been a challenge, the company's financials have been steady, and its strategy for growth and profitability is reasonable and solid. Capitalizing on the loss of trust with US-based products is not a strategy in itself, but should provide a 'foot in the door' for many new markets. While the next-generation firewall (NGFW) market is already fairly commoditized, Clavister has a few technical tricks up its sleeve that should differentiate it from most competitors. The company's size is a concern, with respect to breadth of innovation and R&D capabilities, but as long as it doesn't try to boil the Baltic, it should be able to execute more quickly than the majority of its competition.

Context

Clavister is publicly traded on the FN Stockholm Exchange (under Clavister Holding AB) and headquartered in Stockholm. The company was founded in 1997, and has more than 130 employees. CEO Jim Carlsson came to the company from his position at Intel as VP for network and security business in May. The company has struggled to grow its revenue beyond the $10m-per-year range, and has not turned in a profit for several years. Despite these challenges, company executives point to key strategic product introductions and rationalizations, channel developments, and market entry initiatives underway to turn around its prospects. The company has set a goal to turn a profit sometime during 2015. It has enough cash in the bank to sustain operations for several quarters, but is counting on its new initiatives to bear fruit next year.

The company may have also run into some luck as revelations stemming from the Edward Snowden NSA leaks have worked in its favor. There is a widespread perception, or assumption, overseas that security equipment manufacturers in the US and affiliated countries have been forced to leave open 'back doors' for the NSA and other government agencies. This backlash has opened opportunities in Japan, Brazil and other countries looking for a competent, high-performance replacement – a replacement these countries seem to be finding in Clavister. This same concern for data privacy from government-sponsored espionage has also impacted Chinese network infrastructure companies, with Huawei, ZTE and others being largely shut out of telecom networks in the US.

Products/Services

Clavister has a suite of network security appliances that perform all the functions expected from modern NGFWs, as well as a few less common features like fully configurable offerings with stateless/stateful firewalling, support for both transparent and routed mode, NAT pooling, SLB, DPI, application control, advanced routing, and support for a larger range of VPN types and functions (like VPN stitching) than is typically seen in this market. The company supports these services through a range of integrated hardware appliances, including remote and branch office (Eagle series), industrial (Lynx series), and enterprise and datacenter (Wolf series), as well as central datacenter, telecom and carrier-grade (PolarBear series). The company offers a virtualized version of its network security appliance branded Clavister Virtual Security Gateway (VSG). During 2013 Clavister made a decision to go all-in for Intel x86 architecture (due to scaling, performance and cost), thereby phasing out previously supported computing architectures like ARM and MIPS. Having only a single architecture to develop for will streamline and decrease the cost of software development for the company's varying hardware platforms. Clavister will continue to support end-of-life implementations as customers migrate to x86-based devices.

A key driver for Clavister's products is the global mobile network transition from 2G/3G to LTE networks. This trend is increasing the need for IP security across the network edge, backhaul and core elements because LTE relies heavily on IP networking. The Clavister security gateway has been deployed for 2G, 3G and 4G/LTE mobile networks to protect the SGi/Gi interface and the radio backhaul, sites, roaming interfaces, backbone, and mobile core. The security gateway also provides the ability to control the subscriber authentication, access control and content control (e.g., Wi-Fi offloading). All the above can execute on the same hardware/software simultaneously because Clavister's offerings have no limitation in function – only in capacity – it doesn't matter if it's an appliance or VSG, all the functions are reachable in all execution points.

Performance is a particular point of pride for the company, which claims a high level of efficiency and performance across both software and hardware. Clavister has full control over its product, with its own network operating system (cOS Core cOS Stream). Clavister has many customers using hundreds and even thousands of its products, and built a product called InControl to address centralized management. An SDK allows companies to integrate InControl with other internal systems and processes. The company differentiates from the competition through a combination of its small software footprint (cOS Core weighs in around 32MB storage and 128MB RAM support for specific features such as IPsec for LTE backhauling) and its proven strength in running its software in a virtualized environment. The latest release of the cOS (10.21) introduced several new features, including Service VLAN (Q-in-Q), 6in4 tunneling support and L2TPv3 client support. The new L2TPv3 functionality will make it easier to devise cost-effective alternatives to MPLS services, simplifying application and server mobility and extending the virtualized enterprise over WAN (WAN optimization will be supported in a future release). Additionally, the new release supports nonintrusive SSL inspection for application control, with support for more than 2,300 recognizable applications and 2,400 application metadata tags.

Go to market

The company currently has a near 50/50 split between indirect channel and direct sales, but part of its turnaround plans see it moving to a model more heavily weighted toward indirect selling to telecom carriers through major telecom equipment manufacturers. The target mix is likely 70/30 indirect to direct. The company currently has an OEM relationship with D-Link and Ericsson. It sees its strongest opportunity in penetrating the telecom sector with its products, although it acknowledges that the long sales lead times, test cycles and expected product lifecycles (5-15 years) are vastly different than the enterprise sales model, and are challenging to navigate. The company sees opportunities for its wares at all tiers of telecom operators. It also has a strategic and strong relationship with Intel, and is part of the Intel Network Builders program.

The company has seen some success in Sweden, Germany, China, Japan, Asia and South America, but pulled back from the US market in 2012 due to a lack of resources required to scale business there (although it still has a handful of direct customers). Clavister recently announced that it is collaborating with Swedish IT provider Bluecom to deliver the outdoor secure Wi-Fi network for the 2015 World Ski Championships in Falun, Sweden. The organizers of the event are focusing on maximizing the audience experience with smart Wi-Fi offerings and services for the 200,000-plus spectators that are expected to visit the area during the event, as well as enabling secure, flexible communications for the event's athletes, volunteers, officials and media.

The company has significant market activity in Japan, where it has established a strategic partnership with 8,500-employee-strong Japanese systems integrator MIRAIT. In Brazil, the government was direct about NSA fears being a key factor in decisions to move away from US-based products and companies. Brazil has been outspoken and active about taking measures to prevent NSA espionage activities, including building an undersea cable to Portugal, moving away from Microsoft email products and requiring the government to depend only on domestic IT services.

Competition

Clavister finds itself in a very competitive market for network security products, particularly in the NGFW segment. A sampling of competitors includes Cisco, Juniper, Huawei, Palo Alto Networks, HP, Check Point Software and Fortinet, although it should be noted that the competition in the telecom/carrier niche is narrower than the general NGFW market. Clavister argues that its combination of relative size and nimbleness allows it innovate faster than the competition, and that it is well ahead of its larger competitors in embracing cloud and virtualized architecture, which positions it well in a telecom segment pushing suppliers hard in this direction.

SWOT Analysis

STRENGTHS	WEAKNESSES
A Swedish base and full control over manufacturing and software development will go (and have gone) great lengths toward easing customer fears related to state-sponsored espionage, especially from the US. Clavister has a mature product proven in large environments. Company size allows for shorter development cycles and a more aggressive roadmap.	There are financial viability and strategic-turnaround-execution risks. Company size and long-term future will be concerns with potential customers, especially in markets where sales cycles are 5-15 years long.
OPPORTUNITIES	**THREATS**
Clavister can expand into additional Latin America, EMEA and Asia-Pacific markets via global partnerships. Any countries concerned by NSA revelations represent potential opportunities, as well.	Despite the NSA revelations, US and Israel dominate the network security markets so heavily that Clavister is still facing an uphill battle against years of marketing momentum, certified network administrators and brand-specific knowledge.