AI: as much an opportunity as it is a threat to cybersecurity

Jesper Trolle, CEO Exclusive Networks Group

Les Echos Bourse / Investir

« L'IA est autant une opportunité qu'une menace pour la cybersécurité » | Investir (lesechos.fr)

Your group is not well-known to the general public. Could you tell us about your business?

We are what we call in the industry a "tier 2" player. In the world of cybersecurity, you have, on the one hand, the ISVs (Independent Software Vendors) - the solution developers. These are big companies like Cisco, Fortinet, Palo Alto… And, at the other end of the chain, you have the customers: companies of all sizes, working all over the world and having cybersecurity needs specific to their activities to protect their data. Within this value chain, our customers are these ISVs. We help them deliver their solutions to end users, via an indirect network of partners such as Atos, Capgemini, Orange… Created in Paris 20 years ago, we are today a Group with our offices in 47 countries, selling our products in 170 countries and employing nearly 2 600 people.

Why can't a company work with solution vendors directly, without relying on you?

First, because it's a very fragmented landscape. More than 3,000 companies are developing solutions. And every year, new businesses emerge because the threats multiply. Second, businesses with cybersecurity needs are found all over the world. We work with over 200 solution creators, who sell to 150 000 end customers. If these customers interacted with Palo Alto directly, there would be tens of thousands of requests to process. This would be possible if those only came from the US. But these are companies from France, Spain, Vietnam… Meaning different areas, with different standards and currencies. Having our local offices in these countries, we can understand their expectations. Thus, solution sellers benefit from partnering with us, as it allows them to work with one company that grants access to all these markets. On the other hand, if our model exists, it is because cybersecurity is complex. We help businesses identify their needs and determine the most suitable protection, matching them with the right provider.

After two years of growth of almost 40 %, your development returns to normal (+15% of turnover in 2023). What do you think of this performance?

We are very satisfied because, for the first time, we have exceeded 5 billion euros in sales. It was a real challenge after an exceptional year 2022. 2023 can be divided in two: a first half of strong growth, as expected. Then, demand decreased, in the wake of the economic slowdown and the expectation of lower rates from central banks. In this context, all expenses are carefully monitored. But that did not prevent us from generating cash, which allowed us to acquire two new companies in 2023. First, Ingecom, a Spanish company also present in Portugal and Italy, which is aimed at cybersecurity businesses wishing to become leaders in their segments. And last December, we acquired Consigas, a global cybersecurity services provider based in Europe, specializing in training and consulting.

How do you plan to maintain a high level of growth?

We should see an improvement in the economic context in the second half of the year, which will help revive demand. To take advantage of this, we are identifying several pillars of growth. First, there is the cybersecurity market, which is growing by 8-11% each year. Next, we need to expand our geographic presence with ISVs and work with new vendors. Every year, we sign contracts with ten to fifteen new vendors, which bring long-term growth. Acquisitions will also continue, as we just did in March, with that of Nextgen Group, a specialist in cybersecurity solutions in Australia and New Zealand, very active in a number of services such as lead gen, data analysis, and cloud migration. This is a very important and strategic acquisition, as it allows us to double our presence in the APAC region and become a leader in this market. Finally, we will be able to generate added value through our ancillary activities, such as training and services.

Cyberattacks will cost the global economy $10.5 trillion in 2025, 300% more than a decade ago, according to Cybersecurity Ventures. Are companies allocating sufficient resources to protect themselves?

I don't think we can ever do enough. But every company spends 5-8% of its IT budget on cybersecurity to deal with increasing threats. All companies are affected. As proof, every week, at least one Exclusive Networks employee receives a message pretending to be from myself! But as companies are getting more and more involved, hackers are keeping up as well. They always have more resources, are better organized, and have access to more powerful technologies such as artificial intelligence (AI). If you take cybercrime as an economy, it is the third largest in the world in terms of GDP. All of this must be coupled with a world where we have access to our data on multiple devices, accessible from any location, on a train, on a plane, in a hotel... So many factors that fall outside the protection measures of companies.

What are the main cybersecurity challenges for businesses?

I think that what we call Identity Access Management (IAM) remains central. It's important to always ensure that the person connecting to any device is authorized to do so. This was first done using a password, then with two-factor authentication, and will continue to evolve. In a world where digital technology is ever more decentralized, this is a critical issue. The other key element is about data loss prevention. Today, you can copy any text into an artificial intelligence software like Chat GPT and ask to analyze it. But no one knows where this data goes. Businesses must determine what kind of information can be used in there, and which data must be protected.

How does AI affect cybersecurity?

I would like to say that it is more of an opportunity than a threat, but that is not the case. Solution developers have already integrated AI into their products to improve their performance. This technology also makes it easier for companies to detect threats and improve human work. But hackers have access to this technology as well, and can use it, for example, to quickly write a code that will be able to exploit a flaw in a system that requires an update. The positive effects are numerous, but the negative ones are just as many.

#Cybersecurity #ArtificialIntelligence #AI