ceocfointerviews.com

Issue: May 9, 2016
The Most Powerful Name in Corporate News

Canada's First Cloud-Based Security as a Service Platform for Enterprises focusing on Detection and Response providing Full Visibility Across All IT Assets

John Menezes
President and CEO
Stratejm Inc.

CEOCFO: ***Mr. Menezes, what is the idea behind Stratejm?***
Mr. Menezes: We are building the first Security as a Service in Canada. It is addressing a problem that most enterprises have with security. The problem is that the enterprises are constantly spending a great deal of money on prevention technologies. What we have seen over the last 10 years is that prevention is a failed strategy. Enterprises are spending more money, trying to buy the latest mousetrap and believing they are more secure because they have that latest piece of hardware and in actual fact they are not. Therefore, we feel that enterprises have to move away from thinking only about prevention, to thinking more about detection and response. Our cloud-based services that we have launched solves two problems for them. It addresses detection and response, but it also takes them away from having to constantly spend more money on hardware and software.

CEOCFO: ***Are most companies realizing that it is not as simple a problem as it might have seemed to be?***
Mr. Menezes: The enterprises are sensing that prevention is no longer working. I was at the RSA Conference a few weeks ago in San Francisco, and many of the speakers were saying the same thing. It is that the focus prevention only has failed and we have to focus more on detection and response. The challenge for many security professionals is that for the last 20 years they have been taught and have practiced based on the fact that they have to make sure that their organization never gets hacked. They are mostly operating from a position of fear. If my organization is hacked while I am the security professional in charge of it, my career would be in jeopardy, as I will be on the hook for that. That is the background from where they have been operating. Now with security breaches becoming more common, they are more front-page news, so business people are understanding that it is not an easy solution. The financial folks are also understanding that it is not an easy solution. Therefore, the security people are also understanding if my business understands that it is not an easy solution, and my financial people understand that it is not an easy solution, so maybe now I can go to them and talk about detection and response and less about prevention. Enterprise should focus on reducing the spend on prevention and increasing the spend on detection and response. It means that it is becoming an easier conversation for security professionals to have with their executives, whereas in the past they would have found that conversation to be very difficult.

CEOCFO: ***You have launched Canada's First Security-as-a-Service model. Why Canada, and is this model common in other countries?***
Mr. Menezes: There have been some attempts at it in the US and it is catching on. One of the reasons that we have our service hosted it in Canada is that we have many Canadian enterprises who are reluctant to have their data stored in the US and so are reluctant to use cloud services based in the US. We see that reluctance being acknowledged by Microsoft now announcing that they are going to build datacenters in Canada, for their Office365 products. We have also recently seen Amazon announcing now that they are going to have a datacenter in Canada. We believe that there is significant reluctance on the part of Canadian enterprises to put their data in the US, so when we launched our service we wanted to make sure that everything was in Canada and they could adopt our Security-as-a-Service without any hesitation.

CEOCFO: ***What is your go to market strategy?***
Mr. Menezes: The go to market strategy is quite simple. We are approaching enterprises with our own dedicated sales team. We are approaching mid to large enterprises that want and need to bring their security spending under control and show real results. We are so confident that they will love our service that we are offering what we call a "proof of value". We want them to use our service for 6 months to see for themselves what the real value can be for them, and if after 6 months if our service did not provide value, they are free to go. You made no commitment and there was no capital investment, so all it cost you was 6 months subscription.

CEOCFO: ***There are so many different companies offering a security solution, each having their own different approach. What separates Stratejm?***
Mr. Menezes: Our approach starts with forcing enterprises to back to the basics. That means that you cannot manage or measure what you do not know about. If you go to any enterprise and ask them how many devices they have, the security officer my say that they have 400 devices, if you talk to the network guy, he may say they have 600, and someone else may say 500. Nobody really knows how many devices are being used in the organization, who is accessing data, or the critical assets. With so many unknowns in the enterprise, how do you expect the security team to be able to secure all of those assets or data? Our major goal is to add visibility to everything. Therefore, when we start out we run a number of different scans to be able to identify all of the assets in the environment. We run different scans to be able to understand who is accessing which asset. Then we interview the clients to make sure that we understand the critical assets, and who are all of the privileged users that are accessing those assets. From there we start to monitor and do our investigations. It is really going back to the basics which is often not very sexy but perhaps the most important step. Its much easier to buy the latest and greatest prevention technology and hope that you are protected. But hope is not a strategy. You can go out and spend a million dollars on a solution, but it will not solve the problem long term. Unless you know exactly what you have on your network, how the network is being used, how the assets are interacting with each other, and how your staff are using these assets, everything else will be immaterial.

"Enterprise should focus on reducing the spend on prevention and increasing the spend on detection and response."- John Menezes

CEOCFO: ***What has been the reception so far?***
Mr. Menezes: We have had great reception in the marketplace. We have already signed up 6 enterprises that are between $2 and $4 billion in revenue. We just had an open house and launch which was attended by the Mayor of Mississauga as well as about 65 CEOs and CIO. The value proposition we offer is quite amazing. We are letting them know that they do not have to buy any more technology, hardware or software. We want to just come in and collect all of the metadata that is already being generated in their environment. They can send that to us, work with us, and we will streamline not only their whole security infrastructure, but their whole IT infrastructure. By streamlining it, they will be much more secure, with nothing to lose. Therefore, the value proposition is quite amazing. We are finding that enterprises are gravitating towards this solution, because nobody wants to go out and spend another half million or one million dollars on technology, then find that 18 months later technology has changed, and they cannot adapt. They may also buy technology, but do not have the people necessary to manage and maintain it. There was a recent survey done by KPMG in the Greater Toronto Area, that found for every 12 vacancies in the security field there is only one qualified candidate. This means that even if you do buy the technology and do have the money to invest, you still cannot find the skill sets for people to manage it. You are between a rock and a hard place. Whereas, with our solution you do not have to buy hardware or software. All you have to do is let us leverage all of the data that you are already producing in your environment to help you become more secure, which is a great proposition for our customers.

CEOCFO: ***Are there particular types of companies, sizes or geographies that could use your service?***
Mr. Menezes: Initially, obviously because of our, "Made in Canada, outsourced in Canada", we are definitely targeting Canadian customers. Number two, we are targeting customers that have between 500 and 5,000 employees. That is the size of customers that we believe is our sweet spot. Since our approach to security is the same, whether you are a retailer, healthcare company or constructions, and because we are adopting such a fundamental approach to security, we think we have a great story for any vertical. However, there are going to be specifics, such as in retail PCI will be a big concern for them or in healthcare PIPEDA. If you are working with credit unions or with the banks where they have Sarbanes Oxley and all of the other compliance regulations that they worry about might come into play. We believe that we have a very significant foundational approach that will apply across the board to any size customers, even though we are targeting between 500 and 5,000 employees.

CEOCFO: ***What have you learned from your previous ventures that has been most helpful with Stratejm?***
Mr. Menezes: I ran a traditional Managed Security Service for 10 years before I exited out of that business very successfully. What I learned is that you have to go back to the basics and focus on the fundamentals. Being an MSSP you almost had a conflict of interest because you had to sell some hardware or software to be able to manage it. What we have done now at Stratejm is to take advantage of all of the technology that is out there. Our solution is based on using the cloud, big data analytics, mobile technology, machine learning and focused on automation. What I have learned is that in whatever we are doing, we have to make it simple and easy for our customers to utilize the services that we are providing. In the old world it would take us between 6 and 9 months to onboard a customer. In the new world I can on board a customer in 6 weeks. In my old world, it took a long time to generate reports, and now we have a very good reporting engine, where customers can run any type of report they want without having to call us or ask for it. They can go into our system to run a report quite effortlessly as the user interface is very intuitive. What is important is that I have learned to understand what the customer is looking for. It is easy to use, easy to understand and still reduces their risk, as well as keeps them safe and lowers their cost.

CEOCFO: ***Finally, what might a potential customer miss when first looking at Stratejm, that they really should be understood?***
Mr. Menezes: They really should understand that our service is taking a very innovative and different approach to solving an old problem. It's different in terms of how we are investigating the incidents and our methodology for quickly determining that it is a false positive. We don't want to send our customers a bunch of false positives. The less they hear from us the better. This in itself is a difficult concept. I mentioned that the average dwell time of a hacker is about 259 days according to Gartner and Verizon Breach Report, so expecting response time in hours is not practical but customers have become used to that concept and at Stratejm it is quite different. That whole concept of calling you up in 15 minutes or calling you at 3:00 in the morning to alert you that something is happening is only something that happens in the movies. It is not real life anymore. If you want me to tell you that your server has gone down or there is a DDOS attack I can definitely do that in 15 minutes or almost immediately, because our response mechanisms have all been automated. We cannot report a breach in 15 minutes, our biggest challenge is in informing our customer base in this whole different approach to security, because people are so focused on the just prevention. That is true even with their budget spending, where they are spending 80% to 85% of their security budget on prevention technologies, but we think that number should be no more than 25%. The rest should be spent on detection and response.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

Stratejm Inc.

For more information visit:
www.stratejm.com

Contact:
Laura Regehr
416-305-5747
laura.regehr@stratejm.com