ceocfointerviews.com

Issue: January 26, 2015
The Most Powerful Name in Corporate News

Cyber Security through Math and Machine Learning

Stuart McClure
CEO, President & Founder

CEOCFO: ***Mr. McClure, what is the idea behind Cylance today?***
Mr. McClure: We protect the world's networks and computer systems in critical infrastructure from attack. We do that by protecting the computer itself or the mobile phone. We protect in a brand new, novel way without any signatures or any type of traditional detection techniques. We do it through artificial intelligence methodology. For us, the ability to prevent the unknown is very simple. We simply mathematically represent that which is bad and build the model into our endpoint product that prevents all that is bad from ever executing. We can detect and prevent all the advanced attacks that are coming out today, all the new campaigns that come out tomorrow, and we never need any updating.

CEOCFO: ***How is your approach different? You mentioned mathematics?***
Mr. McClure: The math approach is the biggest differentiator. Traditionally, how security companies work is they have to see an attack happen successfully before they can ever detect it in their product. They have to break down that attack step by step; what the attack did, how they did it, and then they write what is called a signature for it, which says that if we see this activity again in this sequence, in this quantity, then this is bad. The problem with that is the attacker advances their methods too quickly. They change their techniques all the time and they change their tactics. Often, a detection signature that is written today could be obsolete seconds after it is released. What you end up doing is shoveling sand against the tide - you are never going to get anywhere. At Cylance, we have actually extracted that determination of good from bad into a mathematical formula, using machine learning and artificial intelligence to determine whether something is going to be bad before it is every seen in the world or executed. By doing that, you can prevent the attack immediately.

CEOCFO: ***Can you give us a simple example of how that works?***
Mr. McClure: As an analogy, the human genome project. . Ancestry.com has something called ancestryDNA.com. What is will do is take a collection of your DNA from the inside of your cheek and it will break down the DNA and look up in its enormous database of all DNA known to determine your relationship to anybody in the database. If you wanted to know how related you are to George Washington, you would be able to know that. How do they do that? They take the millions of features in a typical DNA strand and map them out one by one. They take your DNA and do the same reverse mapping and marry it mathematically to all that which is known. Here is another example. Let us imagine we are at a café in Paris. People are walking by. You cannot see the people walking by, only I can, and you tell me "Hey Stuart, my brother is in Paris too, would you mind if he joins us for lunch? I told him to meet us here and to look out for you but I cannot see him so you are going to have to look out for him." I ask you to tell me what he looks like and you say that he is tall, skinny, has brown hair and usually wears jeans. I look up and down the street and I say maybe ten people at that time. I say there is no way I can find him out of the ten, so give me more details. You say that he is wearing a beret hat today and he is typically a very fast walker and often has facial hair. Now I get down to about two people and I start to wave to both and only one waves back. Every single element described is a feature. You gave me the physical description of features. You gave me the temporal features of him being aware that I would be looking out for him so he would wave back to me. Similarly, what we do with machine learning on a computer is map to six million features of a bad file. By doing that, we can tell you definitively whether something is malicious before it is ever executed to do harm.

CEOCFO: ***Where are you in development and commercialization?***
Mr. McClure: We started the company just over two years ago and we just released our technology eight months ago. Therefore, we are early in our release cycle, but we already have well over fifty customers on the technology and the

adoption is growing every day. This is because people are fed up with the fact that none of the technologies available and deployed today can detect the advanced threats or even some of the most common threats out there. Organizations have to think differently about how to prevent these attacks today. As the word gets out about our company and technology and as our technology is deployed on more and more customers and nodes, we can prove to the world how effective this technology is. That is when you really start to see a landslide of adopters getting onboard. Just like any new industry, you have innovators, early adopters, late adopters. Right now, the ones that are buying our technology are the true innovators and early adopters, the folks that are desperate for a solution; they realize they have a big problem. Many companies do not even realize they have a problem, which is the first challenge, simply proving to them that they actually have a problem. To encourage them, we say to install us for free for 60 days on 100 of your systems and see what it discovers. If you do not find something that is compelling for you, we will walk away and not bother you. If you do find something compelling, you need to adopt the technology. That has been incredibly effective.

CEOCFO: ***What is involved in implementation?***
Mr. McClure: It is very simple actually. You install a small 20mb agent on the end point that is already preconfigured, so you can do it on thousands or hundreds of thousands of systems at the exact same time. They all connect into our cloud for a policy update and once that policy update is done, that is it. It does not need to be updated again, and it does not need to have constant cloud connectivity- it just needs to be running and protecting the system.

"People are fed up with the fact that none of the technologies available and deployed today can detect the advanced threats or even some of the most common threats out there."- Stuart McClure

CEOCFO: ***How are you reaching out to potential customers?***
Mr. McClure: We are reaching out in a couple of big ways. The first is direct, going to our enterprise customers of the past or those that have come inbound, looking for new innovative technology. We are certainly involving partners as well, including resellers, VARs, system and integrators. These are folks that already have the relationship with these customers that desperately need a better solution, so they are coming to us and bringing opportunities to display the technology. Security is a very small industry and much of it is word of mouth. We try to get out to conferences and shows and through some marketing materials, such as on today's cyber threat report that we just released on "Operation Cleaver". At the end of the day, it is a word of mouth industry.

CEOCFO: ***What about competitors looking to adopt your model or trying to recreate it?***
Mr. McClure: There is always a threat of fast followers that look at what we are doing and think it is great idea that they can do better. We have IP patents (intellectual property patents) that are already issued as well as in process. The barriers to entry for a competitor are significant, because we have broken ground in this industry – we had to solve very big problems that no one else has had to solve and by doing so, we have a huge advantage over anyone that wants to try and get into the game. It is also our deep security domain knowledge and the gravitas that the team brings around security that helps show how we differentiate amongst just about every company out there in the industry. In addition, we know the attack, techniques, tools, tactics, actors, and we know exactly how, when and why they get in and we built that observational power capability inside of our technology to get smaller and smarter every single day. We will never stop innovating and we will always strive to stay ahead.

CEOCFO: ***Are you funded for the push or will you be seeking funding or partnerships?***
Mr. McClure: Right now we are funded to complete satisfaction at this point. We do not need to look outside and we believe we are well on our way to be able to be autonomous.

CEOCFO: ***Put it all together for our readers. Why pay attention to Cylance today?***
Mr. McClure: If you care about your systems and networks from being hacked and you want to actually prevent the attack, we are the only solution that will do it today and in the future through the use of math.

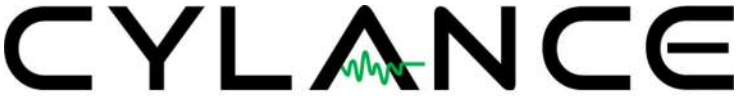
Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

BIO:
Stuart leads Cylance as its CEO and visionary for a new approach to threat detection, protection and response. His leadership sets the strategic direction, operational execution, and fiscal investments of the company. Stuart is one of the leading experts and practical thinkers in the computer security industry today. With a highly regarded 25-year history in the security industry, Stuart has led some of the most notable companies in the space.

Prior to Cylance, Stuart was EVP, Global CTO and General Manager of the Security Management Business Unit for McAfee/Intel where he was responsible for a $3 billion consumer and corporate security products business. During his tenure at McAfee, Stuart established an elite team of security researchers called TRACE, which frequently discovered 0-day vulnerabilities and emerging threats in embedded and critical infrastructure. Before McAfee, Stuart formalized the cyber security program at Kaiser Permanente, a $34 billion healthcare company.

In 1999, Stuart launched Foundstone, Inc., a global consulting and products company, which was acquired by McAfee in 2004. Stuart is the creator and lead-author of the most successful security book of all time, Hacking Exposed. This book is now on version 7. He is widely recognized for his extensive and in-depth knowledge of security, and is one of the industry's leading authorities in information security today.

Stuart McClure earned a bachelor’s degree from the University of Colorado. He also holds a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications. He serves as a member of the Advisory Board at CounterTack and Accuvant.



Cylance Inc.

For more information visit:
www.cylance.com

Contact
Greg Fitzgerald
Chief Marketing Officer
512-413-2211
gfitzgerald@cylance.com