ceocfointerviews.com

Issue: January 16, 2017

CEOCFO Magazine

Signal Sciences Web Protection Platform Stopping Attackers from Breaching Critical Customer Data via Vulnerabilities in Application Code

Andrew Peterson
Chief Executive Officer

Signal Sciences
www.signalsciences.com

Contact:
Andrew Peterson
424-289-0342
Andrew@signalsciences.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"As a defender, you really need to understand what your attacker is actually doing and where they are trying to exploit the problems that already exist within your applications from a security perspective and that's exactly what we do."- Andrew Peterson

CEOCFO: ***Mr. Peterson, what is the concept behind Signal Sciences?***
Mr. Peterson: Forty percent of successful breaches today actually happen through code vulnerabilities in people's websites. It is called application security. Yet, only five percent of security budgets go to that area of security specifically. At Signal Sciences, what we have built from a technology perspective is a web protection platform that is enabling these companies to find and stop attackers from breaching critical customer data via vulnerabilities in their code.

CEOCFO: ***Would you please explain what vulnerability in the code means?***
Mr. Peterson: A vulnerability in the code basically means that when someone is building a website there are bugs in the code. Most complex websites are comprised of millions of lines of code. Imagine you are writing a paper that is one million sentences. Regardless of how careful you are, you are going to have some typos that you need to fix. It is the same thing in code. A typo in a paper equals a bug in website code. And these bugs can actually result in is a security flaw that an attacker can take advantage of to get to data that you do not private and protected.

CEOCFO: ***Inattention because it is not a "sexy" type of breach? Why has it been under the radar?***
Mr. Peterson: The way in which attackers have been attacking organizations has changed over the last ten years, just based on both where these companies have been investing some of the security resources in the first place, but then also the way in which people are changing how they are actually developing their technologies. In the past, a software application would get install from a CD onto your computer itself creating a different vector of attack. Now those same programs are being built as a web application that you would run through a web browser. So instead of installing the program on your computer, you just go to a website and you would actually log in to access all the same functionality. The difference is that because it is via a website, anyone in the world can access that. Therefore, it makes it really great for consumers because they can access the program on their phone, ipad, or home computer anywhere in the world. However, it makes it really great for attackers also, because they can attack you from anywhere in the world as well.

CEOCFO: ***At what level are you reaching customers? Is it at the application website level? Is it end user?***
Mr. Peterson: We are selling to businesses that are running websites and they have data that they are protecting for their customers, so it is ultimately impacting both. We are protecting the company itself, because there is a lot of different types of data that an attacker might be trying to get access to. However, we are also protecting their end users data as well.

CEOCFO: ***Are there many companies working on web application security?***
Mr. Peterson: There has been. There have been many different companies and approaches to application security over the last fifteen years, because websites have been around for close to twenty five years at this point. However, the way in

which technology and websites are actually being developed now is very different that the way it was done in the past. In the past, people would have something called a waterfall development life cycle, which would take six months to deploy a change to a new website. What has happened over the last few years is that a lot of technology has been enabled and created to allow people to make changes to their applications extremely quickly. Sometimes that is even up to multiple changes in a single day. Therefore, as a result you are getting more and more of these bugs; more of what we call application vulnerabilities, being created every day now, where in the past you had six months to find those problems before they actually went to something that was available on the internet.

CEOCFO: ***Are many companies looking for the next generation of web application security? Do they not realize the need or do they think they can handle it themselves?***
Mr. Peterson: That is a good question! I think what is leading the trend here is the changes that allow the engineering teams within these organizations to really increase velocity in terms of how fast they are making changes to the technology that exists in these web applications. That is the most important goal for these companies. So security becomes a bit of an afterthought. However, now people are starting to realize that security of this new generation of web application development is actually quite important. Therefore, we are starting to see more and more customers actually reach out to us about how to solve this problem for they are realizing they have no solution for at the moment.

CEOCFO: ***What is involved with an implementation and what is involved on an ongoing basis?***
Mr. Peterson: This is a really important part of how a lot of technologies in this area have failed in the past. It has been very arduous for people to get started and to actually get something installed into their systems in the first place. That is both because the technology has not been very flexible in the past, but also the past technology has not really been built for the way people are developing modern web applications. Our company and our founders started from learning much of the technology in house for a really large website company called Etsy. From there we learned how important it was to make this process as easy as possible for people to get started. For people now it is literally the fastest install that we had. It went from getting an invite to the platform to installing something on a live production server in five minutes.

CEOCFO: ***What happens day-to-day, what kind of alerts, reports? What will the company get? Will they know when it is happening after you fix it?***
Mr. Peterson: The thing that companies get when they install our software is that they get visibility into the active attacks that are happening on their web application at any given time. This is something that even security experts that we work with at a lot of these companies, and these are major companies; they get surprised at how often and how variable the attacks are that are happening against their applications. They are surprised, really because they have never had visibility into what the attackers are actually doing. No technology has really focused on showing the defender what the attacker is actually trying to do. What companies are then able to do is that they get to prioritize where they are spending their time defending their applications based on where attackers are actually attacking them, which is really the most urgent area to be focusing on for them.

CEOCFO: ***Do potential customers get that right away?***
Mr. Peterson: It is surprising? It is something that we have been kind of wondering; why it has not existed since we started working on this. That is because it seems pretty straight forward. As a defender, you really need to understand what your attacker is actually doing and where they are trying to exploit the problems that already exist within your applications from a security perspective and that's exactly what we do. However, I guess sometimes the simplest ideas are probably some of the best ones; it is just that no one has done it.

CEOCFO: ***Are you working directly with end customers? Might you partner with other companies with other approaches to security or perhaps license the technology? What is your business model and what might it be going forward?***
Mr. Peterson: We work primarily directly with end customers, although security is something where there is a lot of different components to securing a web application. We do not solve all of the security and we do not claim to solve all of the security. However, we try to do the area that we are really focused on, which is layer seven application security. We try to do that particularly well.

CEOCFO: ***What is your geographic reach today?***
Mr. Peterson: We have customers from Europe to Australia to Canada to a lot in the United States as well. Our team is primarily based here in the United States, but we have customers all over the world at this point.

CEOCFO: ***What has changed, if anything, in your approach over time? What have learned as more and more people are using your product?***
Mr. Peterson: I think that biggest thing that has changed for us is the understanding that especially large companies have lots of different types of technologies that they need support for from an application security perspective. What is very important for them is having a variety of choices to choose from when getting this layer of protection installed for them. Therefore, we have been expanding the sort of platform support that we have over the last three years. Now, instead of people having just one option get us installed they have got four or five different options for each type of application that they are looking to install this on.

CEOCFO: ***How do you standout, for example, at an RSA conference?***
Mr. Peterson: The security industry is really hard for customers. That is because there are many different vendors that are there and a lot of the message from a marketing perspective, the words people use; they are all the same. Therefore for us, the way that we really try to help customers cut through the noise there and help potential customers cut through the noise is to focus on allowing our customers to tell their own stories about the value they are getting from our product. For instance; what you want to be able to find in this industry is word of mouth recognition of value being added from a product and that is exactly what we have tried to focus our marketing message on.

CEOCFO: ***How is business?***
Mr. Peterson: It is good! We have primarily focused on trying to build a valuable product and technology platform for the last few years. It has really just been the last year and a half that we have been starting to focus on building our marketing and sales function, to make it so that customers have an incredible service experience with Signal Sciences as well as technology experience. So far all of those things have been going well and we have been able to expand to new customers without sacrificing quality from a technology perspective.

CEOCFO: ***What is next for Signal Sciences?***
Mr. Peterson: What is next for us is continuing to actually bring our technology to more people. The problems and the reason why we started the company in the first place is that the industry is really suffering from poor defensive technology. Most of our goals are based on how do you build a technology that is not just used by the security professionals within an organization, but it really helps to engage people from across the company to help identify and solve these problems as they are happening in real-time. This is something that has been a real problem for the industry and we believe the only real path forward for us to improve how we are protecting ourselves is to have the entire company understand how it gets attacked and be involved in the process of defending itself.

CEOCFO: ***There is so much going on in cybersecurity. Why is Signal Sciences noteworthy?***
Mr. Peterson: We were born as practitioners, so we have had to build solutions to problems in the exact shoes that our our customers are in now. Therefore, we have a pretty deep understanding of the challenges they are up against, the solutions that do not work, and the ones we eventually landed on that do. That is the thing that has really led us to what we have built here. It is really based in a practical approach to the real problems that you face as a defender and that is oddly quite different compared to most of the rest of the industry in security vendors.