ceocfointerviews.com

Issue: October 6, 2014
The Most Powerful Name in Corporate News

Real-Time Active Network Defense Cyber-Security Solutions

Steven Rogers - *CEO*

About Centripetal Networks
Centripetal Networks Inc. is a cyber-security solutions provider specializing in Real-Time Active Network Defense. Centripetal was founded with one vision: to protect the Internet at the scale of the Internet. Centripetal has brought together a team of individuals with backgrounds firmly rooted in cyber, both commercial and the defense and intelligence sectors. The Centripetal Networks team is comprised of experts from Verizon, the Department of Homeland Security, the National Security Agency, the Department of Defense and many other leading cyber organizations. In addition the company has made it their mission to manufacture a complete product for intelligence-based cyber defense. Through their combined efforts, the Centripetal team was able to engineer and bring to market the first scaled real-time active network defense solution.

Centripetal has achieved several breakthroughs in the scale and speed of network protection. Centripetal's RuleGate® product is the first and only system able to action threat indicators at scale, at full line-rate speed, and with agility. Threat intelligence can now directly drive an active cyber defense without negatively impacting network performance or user experience. Centripetal's offering includes the RuleGate® a unique ultra high performance network appliance, QuickThreat™ the industry's first real-time threat visualization and analytics platform, and the Advanced Cyber Threat (ACT) service.

In addition to consistently being on the cutting edge of cyber defense, Centripetal Networks is devoted to engineering and manufacturing their products in the United States. This commitment provides superior supply chain control for the Centripetal's products and conformance to security and performance specifications.

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

CEOCFO: ***Mr. Rogers, what is the concept at Centripetal Networks?***
Mr. Rogers: The concept of Centripetal is to bring the idea of threat intelligence to the practice of an active cyber defense. If you take a look at the history of cyber security, where we have been and where we are now, it is pretty clear that after spending billions of dollars and training lots of people to deploy various cyber defense appliances, we are still having the same problems. We are still not adequately defending ourselves. It is really amazing. Typically, with other product categories, new technology is created to match the challenge and that technology is largely successful. That has not been the case in cyber. The team here, at Centripetal Networks, has identified that the missing element in previous cyber threat intelligence appliances is that they were unable to scale sufficiently to address the problem. We have made it our mission to create a device that can do just that.

CEOCFO: ***What is it that you understand fundamentally about the problem that perhaps others do not and that has lead to a solution?***
Mr. Rogers: What separates us from anyone else is that we can operate on the threat intelligence at scale. I will give you a simple example. If you know there is a bad guy sitting out in Iran or Venezuela or some other region that you believe to be a threat to your network, you can find out who he is by looking at successful attacks he has done. Now you know where he is, what his IP addresses are, his identifying information and then you can say, "Let us write rules that we put into our security infrastructure that keeps him out." Because we do not want to do business with this guy who is attacking, there is no reason that we should not block him from using or accessing our network. It is effective.

Now, every time he tries to enter your network, he cannot get through directly and you can stop him. However, the problem quickly arises that there is an overwhelming amount of malicious threats that need to be blocked. With each incurrence, a new set of rules must be written to stop known threats from entering your infrastructure; with every additional one of these rules that you add you actually slow down your network a little bit. If you go after many attack

sources, you will slow down the network so much that you cannot accomplish any work or the attacker may say, “Okay, I will use a little bit different vector,” and try coming at you again through a new hop and you have to identify and write a rule for that. Then there is too many, which could negatively impact your network performance. Pretty soon, you are overwhelmed with vectors; there are just too many. The existing firewalls and protective systems are just too limited to deal with this. Therefore, an effective threat intelligence defense has not been practical previously.

CEOCFO: *What have you figured out?*
Mr. Rogers: We decided that we needed a fundamentally new technology for evaluating security decisions. The goal would be that we could operate at a very large scale and we could do it without negatively impacting your network or user experience. We saw that we had to remove the processing restraints. To accomplish that, we needed new computer science and new algorithms that would allow us to do many complex comparisons at a very, very high speed. Therefore, we focused first on the development of this new technology. We solved the problem by inventing new algorithms for making analyses and by building new hardware to support those algorithms; and then new applications to make use of the new capabilities. The next step was to recruit many industry leading threat intelligence providers that could populate the system with the known threat actors. This resulted in total enhanced cyber awareness. Now, we can run at a scale where we can put every known attacker on the planet into our system and stop them before they send you the malware, before they sends you the attack and stop a theft before it happens.

CEOCFO: *That would be the time!*
Mr. Rogers: The way threat intelligence is used now, is that you look and study historical data and try to figure out who stole from you last month or last year. Once you identify it, then you have to report it. However, there is not the concept of ”How about we stop that before they attack you, before they steal something.” Now, we can change the tables entirely and can enable organizations to block, alert, or allow cyber threat in real-time, before the theft happens.

“The concept of Centripetal is to bring the idea of threat intelligence to the practice of an active cyber defense.” - Steven Rogers

CEOCFO: *When you present your product or theory, do people believe? How do you overcome the skepticism?*
Mr. Rogers: Skepticism about the solution we bring can be addressed pretty easily. This doubt comes at several levels. The first area of skepticism is, “Okay, the fastest firewall I can buy and pay the most money for can only do maybe a few tens of thousands of rules at the very high end. To do an effective job of threat intelligence-based defense you have to be able to do millions or at least a million rules. “You are saying that you can do that with these specs? That is impossible!” Yes, we do get that a lot. It is very easily dealt with. We can show test reports. We can show the system deployed at other customers or we can help you to test it yourself, with your own test equipment or with ours. We have done that so many times now that I think we are pretty much able to overcome that skepticism.

Another doubt is around threat intelligence. “Can I rely on it? Will I implement faulty intelligence and inadvertently block an important connection, required by my business?” I would say that the threat intelligence industry has made tremendous progress. There are now over 40 companies engaged in the threat-intel world currently. In addition the community now includes government, law enforcement and great collaborations such as the FS-ISAC (Financial Services Information Sharing and Analysis Center). You can just take the “You absolutely must block” threats and implement them in your network. Your organization will save so much work and trouble. Our risk is reduced tremendously and it is unlikely you will get a trouble call.

CEOCFO: *How so?*
Mr. Rogers: As I said the key is that we have done the tests and certifications with a large number of customers in their labs and on their live networks and they were able to see what the results are. They were able to validate or verify that it really does do what we say it does. The larger customers already know they should be blocking known threats, both inbound and outbound. They haven’t been able to do it effectively before.

CEOCFO: *Where are you in the process today?*
Mr. Rogers: We have primarily been focused on product development over the past few years. The company just released a full system product this summer. That product is now past numerous trials and tests as a system with very large customers, both government and financial institutions. It has worked very well. We are now going into large deployments for significant institutions.

CEOCFO: *You have a number of different products. What are some of the variations?*
Mr. Rogers: We have our first system on the market now, which consists of high-speed appliances. Those are the computers systems that we have built that can operate over 1,000 times faster than any other cyber defense device on the market today. Second, we have software that manages and operates those systems. This software system will

instantly update any new threat that they or we know of. Third is also a software product, which is the analysis and reporting system. Since we collect at the moment of attack, then we can also tell you instantly who is doing what to whom. We call this software QuickThreat™. This is a capability that never existed before; it is very amazing. Therefore, if someone comes to attack you, we can show it pop up on the screen immediately. We can show the system stopping the attacks as they happen. Fourth, we have threat intelligence. This data comes from many of the threat intelligence vendors who are out there searching for specific kinds of threats. They are very good in their areas of expertise and deliver this intelligence back automatically to our system. The customer can then procure it and deploy it automatically in their enterprise. That makes the whole system. We also have different speed options, 100, 1G, and 10 Gigabits per second operation.

CEOCFO: ***What is the plan? How are you deploying? What will you be doing for the next six months or year?***
Mr. Rogers: For the next six months we are doing our first large deployments. We are doing them from two different directions. You can deploy the system in your enterprise. Therefore, if you are a large financial services company you can put it on the entry and exit to every facility where it connects to the Internet. That is where you can catch these problems. We are also very interestingly, deploying it in the network with ISPs. This fall we are doing our first scaled test of a service that we call CleanInternet™ with a large ISP, for a large financial services customer. What this service does is it substantially cleans up the Internet that comes to your facility. You get the same Internet that you had before, except it does not have the large number of the most prevalent attackers. CleanInternet™ has a bonus in that it can also free up a significant amount of your bandwidth that is currently used up with attack traffic or even spam. There is much more to say about CleanInternet, but that is basically it.

CEOCFO: ***What have you learned from previous ventures that translates here and has been most helpful in setting the course, knowing what to do or perhaps what not to do?***
Mr. Rogers: If you are at all reflective, you learn many of those things that you just alluded to. I would say of things to do: first, engage with customers as early as possible, even long before you are actually going to sell them anything. That is because the better you understand their needs and problems that they are dealing with on a daily basis, the better you will be able to meet that need and solve the problem in an actual product. The second thing is to carefully manage your application of capital. That is the thing that every entrepreneur needs to pay attention to. You do not want to take capital too soon. You do not want to take it too late. You need to be in a band that is appropriate to what your activities are at the time. For instance, you do not want to be doing a lot of advertising or pushing when you are still building fundamental technologies. Therefore, I would say timing of and the application of capital and the engagement with customers are two of the most important things. Of course, the third one that everyone mentions is that you need to have the right team. You need a team that is capable of doing all of the different jobs that put together a real company.

CEOCFO: ***I would imagine that people are quite excited by what you have developed!***
Mr. Rogers: Yes they are, because as I mentioned in the beginning that as an industry we are not at a mature stage here in cyber defense, even after ten years or more of cyber products; we do not have a ninety nine percent solution. We just do not. We do not have some industry leader where if you just buy their box then most of your troubles go away. We do not have a best practice that you put this in and you are in really good shape. That is very unusual for a technology industry. What we believe is that you can now demonstrate mathematically and operationally what can become a ninety-nine percent solution. Our goal is to make cyber what we call a six-sigma problem. That means that successful cyber attacks become extremely rare. Right now it is unfortunately all too frequent and common.

CEOCFO: ***Will you be seeking funding now for the next steps?***
Mr. Rogers: No, we are not seeking funding presently. We have sufficient. However, we probably will again within the next twelve months.

CEOCFO: ***Why should people pay attention to Centripetal Networks today?***
Mr. Rogers: Cyber is a real threat. We cannot continue to operate where the problem does not get solved for much longer. That is because consumers and business enterprises are gradually losing confidence in the Internet as a means of executing transactions. When it comes to the point where people are individually being attacked and stolen from to the degree that large and well-funded organizations are today, it is going to cause people to pull back from the Internet. That would have disastrous consequences. Therefore, this problem is a “must solve” problem from many dimensions. I think that what is going to happen is that this threat intelligence approach is going to represent a fairly big shift and breakthrough in the whole practice and effectiveness of cyber security. We will be seeing this capability show up on everything from large enterprises and large organizations to ISP services that will be available to you at your home. Think about the long term. How are we going to solve this problem for the user who does not have the resources of a large defense contractor or the government to protect themselves? How is that going to work? Are you going to put a one million dollar cyber defense inside your home in the basement and try to manage that? No. It is not going to work. However, your service providers can provide that and others can do that for you and do it at a much, much lower cost; a cost that is like having some other service such as a video service or something like that on your network, on your ISP.

BIO: Steven Rogers has more than 20 years of technology leadership experience. During his career he founded and served as CEO of 4 network product companies: Cryptek, Inc. (secure terminals), Objective Communications, Inc. (video switching), Cetacean Networks, Inc. (advanced routers), and Rivulet Communications, Inc. (real-time video networks). He has raised over $100m in venture capital and had a number of successful public offerings and company sales. His background also includes management and development at Unisys, American Satellite, Harris Government Systems, and COMSAT. Steven began his career in the USAF, where he worked on new secure communications systems for the AWACS, National Military Command Center, various space-based systems and Air Force One. He was awarded the AF Commendation and the Defense Meritorious Service Medals. Steven holds a Bachelor of Science degree in Electrical Engineering from Virginia Tech. He is also the owner of over 10 U.S. patents.

Centripetal Networks

11720 Sunrise Valley Drive
Suite 100
Reston, VA 20191
571.252.5080
www.centripetalnetworks.com