LeadingAge™ New York

REPRINT FROM FALL 2016

Cloud-Based Threat Detection

Discussion with David Moufarrege, CIO, St. Ann's Community and Sanket Patel, CEO, Securolytics, about St. Ann's Community's new cybersecurity defense system.

Adviser: What precipitated St. Ann's decision to look into this integrated cybersecurity solution?

David: Other highly regulated industries have been addressing cybersecurity for years. In our industry, particularly in New York, there are now specific requirements for Performing Provider Systems (PPSs) under the Delivery System Reform Incentive Payment Program (DSRIP) when it comes to the exchange of data and what they expect from their exchange partners from a security perspective.

In the Rochester area, we're expected to not only report on actual breaches but also trace back potential breaches. Did you have port scans or other types of threats? We started there and looked to see what actually comes in and out of our network and that grew into this more comprehensive solution.

We began working with Sanket Patel and Securolytics about three and half years ago. We started with email archiving then began using their services for email encryption to securely transmit data to the insurance carriers and health systems. Now we have one integrated security solution that reaches across the board, whether it's threat filtering for malware, detection of port scans or other defense mechanisms.

We can now tell you who accessed the network, from where and what they did. If you are concerned about information leakage it can be caught here. This is really important forensically and as a preventative measure. The unique solution that Sanket's team has built really fits into our space and off-loads a lot of the concerns from us.

Adviser: Give a little background about the company.

Sanket: Securolytics is a cloud based threat detection and analytics platform built for IoT (Internet of Things) devices. We address gaps in perimeter-based defenses by identifying the symptoms of a data breach, malware infection and criminal activity through behavioral analysis and anomaly detection. And we do it all without the need to deploy additional hardware or software.

Unlike traditional solutions, Securolytics uses advanced statistical modeling and machine learning to independently identify new problems, learn from what it sees and adapt over time. We reduce the effort needed to discover threats inside your network.

We're based out of Atlanta and we have 250 customers in the United States, across all verticals. About 60 percent of our business is derived from the healthcare vertical, both acute and long term care.

Adviser: Talk about the cost versus benefit. Is this solution something you think should be standardized across the long term care field?

David: I believe so but it's a difficult thing to quantify because it's a question of approach. Number one, we have a solution that does not require you to have an extensive internal IT department. But we do. St. Ann's is actually the third largest healthcare system in the Rochester market after the two acute care systems. So even though we have the scale, we still opted for something we don't have to do internally. It gives us the ability of upgrading without having capital investments or expensive personnel time involved.

Then you have to look at it from a security perspective. Yesterday, I shared an article about a breach at a specialty hospital in Georgia. Those guys ended up going out to the 200,000 patients that were breached and told them, "We're not going to do anything for you in terms of credit monitoring because we can't afford that." So when you start looking at it from a straight business perspective, how do you quantify the damage to your reputation? There are already reports that there are a bunch of sharks threatening to file class action lawsuits against this place. From my perspective, a proactive approach that includes technical security, education and cyber risk insurance would have prevented the situation all together. So there are benefits that you

(Continued)

may not be able to quantify up front but which are equally important.

Adviser: Can you talk about pricing and how to replicate St. Ann's approach?

Sanket: Let's talk about it from the perspective of point solutions versus an integrated approach. There are a couple of ways that it is typically priced. One model goes by the number of users but when you start looking at some of the reporting and the volume of data being processed and stored, it [the pricing] is actually based on that volume, so you have a hybrid pricing model.

St. Ann's has been this amazing customer that got to this progressive solution over time. We put in an encryption update,

[at Securolytics] to kick-start your organization and give you this quick entry point into the solution and give you visibility into your environment. It is called Zero-to-Secure. What Zero-to-Secure does is it actually consumes your organization's logs without any engineer intervention. Within 10 minutes of installation the organization will see its own data and whether or not they have ransomware, compromised devices and insider threats. It also provides device and user details when threats are discovered. The total package price for Zero to Secure is $2,000.

Adviser: What are some of the lessons learned from point solutions versus an integrated strategy?

David: I have been here [at St. Ann's Community] five years. I've run technology across different industries and what I've found is that in general, the point solutions they want are a firewall appliance in the server room and a SPAM filter in front of their mail server. That was basically the whole way of doing this.

For St. Ann's, Securolytics is really not a point solution but rather an integrated approach. We had a firewall in place, we had an anti-SPAM filter, we had an appliance that would do some of the email archiving. Then we wanted to do email encryption. So we did what every other good company does and we went out and implemented ZIX as a solution – that's what MVP and Excellus used. Now we had another point solution. Then we started looking at these fixes and saying, "Wait a minute, there's a capital investment every single time we do this. There's a server administrator that actually has to look at these things and keep them up to speed every time." We still had to contract for expertise from the outside and we still had develop our people by sending them off to seminars and so forth, but we didn't have a view of our holes or gaps. We didn't know what we didn't know!

So we went out and started putting this umbrella around the network and every one of those point solutions was moved up to the Securolytics cloud.

So now I have the same email I'm filtering but SPAM is also being filtered for antivirus in the cloud, it's being looked at from all security perspectives. Does it contain a "payload" of some sort of CryptoVirus? What does the traffic look like in general? So if my colleague is doing some research in marketing, he can use any website and it will be filtered. Now I have a holistic solution that keeps track of all of those things so I know where my threats are coming from.

Sanket's organization provides me with a security dashboard that shows me what goes against my firewall but also what my colleagues and I, in our daily browsing, might have encountered. That helps forensically to keep the network secure and it allows me to focus on other things. The amount of work involved has significantly decreased. We just did a security assessment from the outside and it came out really good for our type of organization. We came out smelling like roses! It was another really good view of the security pieces St. Ann's provides, which ones our ISP provider delivers and the pieces being provided by Securolytics. I feel pretty good that my CEO's not going on the front page of the paper tomorrow because we had a data breach!

As an organization you have to think about what you want to focus on, such as being able to deliver the highest possible clinical outcome and experience for our patients. IT needs to focus on supporting our clinicians, not on keeping the bad guys out as our main focus. That's why I use Sanket's organization.

The one other thing that is important to note is that many of the security processes are cross-industry. They are not unique to healthcare, to senior living, to post-acute care, however you want to define it. So the important lesson is that we need to learn to transfer these processes from other high-risk industries. That's the other piece that an outside solution like Securolytics can provide. It gives you the ability to look at what is truly best in class, what is the best process, not just what the organization across town or down the road does but what national and international companies do.

Sanket: One other thing to add:

securolytics™

(Continued)

Because other customers are using our platform, we can aggregate the data and then report back the "risk slope". We have the ability to take your company, compare you against your peers and assess the risk score – basically, comparing you on your security postures.

Adviser: Other members likely have some security solutions in place already. If they were looking to integrate a full solution, how would they go about it? What's the first thing they should do?

Sanket: Zero-to-Secure is the starting point. It is quick and easy because it is non-invasive. Our claim is that in ten minutes you can have your data in our platform and we can show you where your problems are. You can actually see what we're finding, whether it's ransomware or compromised IoT devices. In the medical field, it could be a medical IoT device that the network administrators didn't even know was on their network, let alone that it would actually go out to the internet hoping to get malicious data in. Within ten minutes the organization has the ability to log in and access their executive threat analysis.

Adviser: Is St. Ann's EMR integrated into the solution?

David: It sits on top of it so that when Securolytics reaches out, it will see our EMR. But there is no need for it to be integrated in the traditional sense because it uses the log files of the EMR servers.

Adviser: Would you recommend that an organization start with a full risk analysis since there is the issue of cybersecurity and HIPAA compliance and there is quite an integration between the two?

David: There is and we're doing the HIPAA compliance assessment for our organization as well. You cannot reasonably do the risk assessment around the security rules without having the data that Sanket's system provides. Now if you go through and use a system like HITRUST, the common security framework for the healthcare industry, it will step you through it. It will ask, "Did you do such and such, what are using for encryption, what did you do for port security, what's your firewall, when was the last time you looked at your server configuration templates?" A Zero-to-Secure type solution makes this an ongoing effort, not just once a year with a huge effort to go through and answer all those questions. You see it all the time through your dashboard, you see it proactively through alerts. You see it all the time.

Adviser: What is the first thing to do if looking for an integrated solution?

Sanket: A few first steps to look for in an integrated solution would be unified reporting, ease of deployment and activation of additional modules and support accessibility.

Adviser: So in terms of lessons learned or things you would do differently, it sounds like the greatest lesson learned is that you would have integrated more solutions more quickly?

David: That's part of it but I think we need to take a step back and remember that everybody starts from a different base level. We are in an industry that was relatively unsophisticated when it came to technology utilization compared to other highly regulated industries. You also have to assess your view of technology. Do you consider it tactical or strategic? I would submit that technology is a strategic asset in today's healthcare and senior housing environment. So IT and IT governance need to be treated that way.

As a result, you first have to assess where you are and what you want to accomplish. Remember that a lot of these security solutions are brand new. What Securolytics proposes – there is simply nobody out there doing what they do. There are companies doing similar things, they have some overlay. But especially when it comes to New York State and the typical size of our senior care organizations, most of the solutions out there are monetized much heavier and geared toward much larger organizations with a much larger IT staff. The solution that Securolytics offers is not something that would have been available five years ago in this form and sophistication level.