NETEVENTS
2015 CLOUD INNOVATION SUMMIT

DRAFT

In the HOT SEAT:

Endpoint Security Renaissance – Cylance Takes on the Global Cybercrime Elite

Glenn Chisholm

CTO, Cylance Inc

Thank you. My name is Glenn Chisholm. I'm the CTO at Cylance. Cylance is a relatively new company. We founded it in 2012. Our focus is endpoint security and obviously we're different in many respects to the panellists that have been up here previously. We are less than three years old and we're doing something, I think is fairly new. Prior to Cylance I was running security at Telstra, which is obviously a telco. And in this audience most people should know who Telstra is.

So what does Cylance do? Cylance builds products for the endpoint. Our focus is providing security, providing -- so Cylance builds products for the endpoint; we build products for the endpoint to protect against malicious activity, in particular malicious software. And why do we think this is important? We think this is important because when we started the company we entered a market that was effectively stagnant with respect to innovation and that is problematic. And, in particular, it's problematic because the attackers innovate very creatively and very frequently. There is a large amount that you would consider mundane, boring, very [inaudible] sort of attacks that one would see, but, at the same time, you also see a great deal of very innovative, very creative attacks against corporations, whether they be from government -- and unfortunately government does participate in these activities -- or whether they be from criminals.

So Cylance has basically built a very different approach; we don't build signatures, we don't build based upon what was there. Our entire methodology is based on building mathematical models that allow us to look at every single binary before it runs and make a decision, should we allow this to run or shouldn't we? And that's done taking advantage of modern cloud computing structure. As a small company I don't

necessarily have tens of thousands of servers or petabytes of storage that I can easily manipulate, but modern cloud computing gives me all of that. It gives me the ability to build the product that we build and to access the compute that we need to build the models that we use in the product.

So we use a number of different approaches. And our key focus is being able to be very fast, very light and provide protection at the endpoint. And so the focus of this discussion is why endpoint, why does endpoint matter? And for a lot of years we saw a lot of discussion about what security can be delivered for the network; you don't need to worry about the endpoint. Any security architecture that misses a key component of the architecture isn't security architecture; it's a piece of marketing. If you don't protect from end to end you've got a problem and the problem is going to be substantive. And in the last few years we've seen the effects of poor security architecture, poor security practice and a lack of understanding of the security environment. And that has been the repeated breaches we've seen, whether it be retail, whether it be healthcare, or whether it be government.

So ultimately I'm not here to shill a product; just to talk about the environment. So, please.

Mankek Dubash – Editorial Director, NetEvents

Thank you very much. There's a lot there that you haven't said. So first question is, a lot of security technologies have come and gone over the years of NetEvents, 19 years of NetEvents, not the 378 I said earlier. I was kidding. We've seen a lot of security technologies come, we've seen a lot of security technologies go and yet we're still plagued by cybercrime. We've got governments around the world getting rattled, Obama and so on, talking about what we're going to do about cyber-terrorism, cyber attacks and so on and so forth. It's a global problem. So how is what you do going to solve or at least go some way towards solving that problem?

Glenn Chisholm

So, I mean I think a key problem with security technologies is they've been very backward looking and the idea that you can protect using what you've seen previously is problematic because it makes an assumption that the attacker is static. If the attacker is static, your problem is really non-existent. And that may certainly have been the case 20 years ago when you started these events, but it certainly hasn't been the case for a substantial period of time. I think, in addition, what we saw for a very long time was substantial under-investment. And the under-investment was not only from corporations but also, quite frankly, from the innovation community. Some of that has reversed in the last five years; you've seen a substantial number of new start-ups, innovative approaches, and you see some of that lack of innovation. You get companies like Palo Alto being created and the creation of this concept of next generation firewall that's moved that market through. And we think that creating this concept of the next generation endpoint that can substantially move the market is really important. No single technology solves a problem, but, as I said, having a

robust security architecture makes a substantial difference. And not assuming the attacker is either foolish or ignorant is important.

Manek Dubash

So what about all the other things we've been talking about today. We've had a lot of things; we've talked a lot and heard a lot about open source and standards and all those things and none of those things seems to apply to security generally or even to your company.

Glenn Chisholm

Open source and standards are certainly important. And we've seen, certainly seen attempts to create standards, whether it be HIPAA or PCI in the security industry. And those standards are slightly different in the way in which you would talk about an MEF standard with respect to [product] integration or orchestration. But one of the key problems is that a clearly describe standard gives a clearly described architecture for the attacker to walk past. If you give a clear set of instructions to the attacker to walk past, they will certainly take advantage of that. And so one of the problems that everyone needs to be very apparent is that while we can innovate, the other side innovates as well. And you can't assume that the other side are two-bit hoods. Most of these people have substantive, high-quality educations and are willing to apply that to achieve a goal.

Manek Dubash

Okay, thank you. One question I couldn't help thinking of as you were talking was the fact that you mentioned that you are lightweight, but still there's a tendency still for software to suck up all the CPU there is available. Endpoints are now mobile, they're now tiny things around ARM processors and smaller; there isn't a lot of CPU available. How are you going to deal with that?

Glenn Chisholm

There isn't a lot of CPU comparable to say a desktop, but the CPU on an iPhone is certainly more impressive than the CPU on my desktop was probably about eight years ago. So everything is relative. We are lightweight; I mean when you look at a collection of signatures you might receive from a traditional signature based approach, that might be 250 meg. We can build a model in less than 35; because I've built a model in less than 35, I can do things in a single pass. I don't have to repeatedly apply signatures and repeatedly search for content. So you can certainly improve performance and improve security at the same time and this is about design and a change of approach. That anti-virus approach is [inaudible] all at this point. And companies have continually applied that base approach and attempted to fiddle with the edges and fiddling while Rome burns is not productive.

Manek Dubash

Now we're in a conference where we've seen not just a lot of technologies but an awful lot of companies come and go. We've seen a lot of new companies be bought by bigger companies. So the obvious question is when are you going to get bought?

Glenn Chisholm

So Stuart McClure, myself and Ryan Permeh, when we started out on this journey -- I don't think that any of us want to get bought. We've all worked in big companies --

Manek Dubash

They all say that.

Glenn Chisholm

I agree. So we've all worked in big companies and we've spent a lot of effort to get ourselves to the point we are now. And we're attempting to create a series of products and a product portfolio and not simply a point solution. I can't speak for the Board, but I want to build a company that makes a difference, not just simply a product that gets bought by somebody else who destroys it.

Manek Dubash

Fair enough. What do you think? Questions. No one has a question for this man? I'm amazed. So how does it work. Tell me more about how this -- tell me more what's -- there is somebody; I beg your pardon. Solange.

Solange Belkhayat-Fuchs - CNIS Mag

Solange, Editor in Chief, CNIS Mag, Computer Network Information Security, a French magazine and its website, written in French sorry. What I wanted to know is how do you do in such a competitive world, because the endpoint security you have so many competitors already on the market well known and all over the world.

So how do you want to have -- how do you do on such competitive market? Just -- are you waiting to be bought by a biggest company or just what --

Glenn Chisholm

We've got quite an aggressive go-to-market, we've got quite an aggressive sales structure to get out there and sell our product. We're two and a half years old and we're well over 100 customers. How do we do in such a competitive market? It's far easier to compete when the competitors have chosen to stay static. I mean, where you've seen a market that's been static for a long period of time, where you've seen a lot of these products that have been used in these major breaches where people have suffered substantive loss, it's a much easier conversation to have than say it possibly would have been five years ago, but it's certainly a conversation you can have with these organisations. And a lot of organisations, whether they be big or small, are looking to restructure that endpoint. I think they took a default position for a long

time and they said, well, if we just do what everyone else does, we'll be okay. And then they realised they wouldn't be; they actually had to do something different. And we're seeing the benefits of that additional -- the additional movement of people into the security space, the additional innovation and the desire for those people to make a difference inside their organisations.

Manek Dubash

Questions. Any more questions? Wayne.

Wayne Rash - eWeek

I'm Wayne Rash with eWeek. So we've heard a lot of vague references to Cylance and their product that you don't want to hype. But I for one would at least like to get some ideas instead of talking about endpoints, what is it exactly that you do for endpoints and how is it exactly that you do it?

Glenn Chisholm

What do we do? We provide the ability for that endpoint to be able to make decisions on what runs and what doesn't run. So you're sitting on an endpoint -- all of you are sitting on endpoints right now, in other words your laptops or whatever device you're using, every time that device executes something do you know whether it's good or bad? It's a very difficult decision to make. It's a very difficult decision to make to what executes on that computer and how it gets there, whether it comes from an email, a web page, a USB stick, a CD, whatever. So being able to make that decision, being able to make that decision in a way in which you're secure is a complex thing. So what do we do? We provide the ability for a piece of software to sit there and make that decision for you. It's should this thing run or is this thing malicious? And it does it for software that it's never seen before. It's effectively a machine-learning built model that uses those -- the technology that you would have seen that -- one would expect to have seen with Google Drive in the car down the freeway without a driver in the front seat, if you've seen algorithmic trading; the ability to make a decision that says, I'm going to look at this thing, I'm going to understand what this thing does and I'm going to decide whether this thing should run on this computer right now or not. And if it isn't good, we don't let it run.

Manek Dubash

But sometimes -- certainly the software I've run from a security perspective, just picking up on Wayne's point, is I get way too many false positives.

Glenn Chisholm

You get way too many -- from running AV?

Manek Dubash

No -- well, I mean, running AV, but also running applications.

Glenn Chisholm

So it's not normally AV's problem. But false positives can occur but in a normal environment one would have a fairly substantial number of files on their endpoint. False positiving wouldn't be a problem on a standard desktop environment. But where you've got this change that one gets, you're constantly downloading software, you're uploading software, you're making changes, it's important to be able to make these decisions and decide what runs. And the issue at hand here is that software using truly interesting attacks has never been seen before by anyone, ever. And more importantly, it isn't re-used in other organisations. A sophisticated attacker doesn't take a piece of software and use it in organisation A and use it in organisation B. They may re-use some code, but code re-use is a complex thing to decipher if they're smart.

Manek Dubash

Okay. Questions? Well I've got one more and then I think we'll probably wrap. What's your reach to market; are you selling to end users or are you selling to service providers or --

Glenn Chisholm

We sell through a few channels. We certainly sell through MSSP and we sell direct to large enterprise. So those are our primary -- we're not a consumer-focused organisation. We're an enterprise focused -- this is primarily an enterprise problem. AV will certainly do a lot better on a consumer desktop than it would in an enterprise where you have targeted attacks. So that's our primary go-to-market and that's the path we're using.

Manek Dubash

Okay. If there are no more questions? Okay.

Rob Ayoub - NSS Labs

Rob of NSS Labs. You mentioned managed service providers and it's been one of the recurring themes in some of the panels is security delivery in the future. So maybe you can talk a little bit; with your current interactions with, call them service providers, MSSPs, how do you see that evolving when we talk about putting workloads up in the cloud? How does that correlate to what Cylance does and to all -- primarily you've been seen as endpoint focused, but how do you address that when you're coming from offering it as a managed service or through a managed service provider or through a cloud provider?

Glenn Chisholm

Yes. The issue at stake is whether or not enterprises can manage their own security and their ability to access staff and create teams that can. And that's a really, really complex problem. Access to human resources is difficult. Managed service providers provide, for a segment of the market, access to that resource capability to allow them

to actually understand what's occurring and to be able to make good decisions, because you can certainly get a file that you think is good, that looks good in every respect and say, no, this is definitely a false positive, click on it and then regret that several years later when you find out you've lost everything in your organisation. And the issue here is is that's not an exaggeration. When you start to look at the concept of dwell time, in other words how long has this malicious piece of software been inside an organisation, how long has it been transferring and exfiltrating information, we certainly see software that's been in there north of 400 days. And so managed service providers that can provide a broad, holistic solution, provide a really important value. And our solution -- I've got a telco background, our solution was designed to a large extent to be able to enable that environment, to be able to enable them to manage a number of customers from a single location.

Manek Dubash

Okay. Glenn Chisholm, thank you very much.

Glenn Chisholm

Thank you very much.

[End]