NETEVENTS

EUROPEAN MEDIA SPOTLIGHT

FINAL

Conference Debate IV: Tools, Techniques and Technologies for Protecting the Endpoint

Analyst Chair:

Alan Zeichick, Principal Analyst, Camden Associates

Panellists:

Steve Broadhead	Founder & Director, Broadband Testing
Carl Gottlieb	Consulting Director, Cognition Secure
Roark Pollock	SVP Marketing, Ziften

One of the earlier presentations gave me the thought that 15 years ago, 20 years ago, if we talked about setting up security for that hairdresser, that small business, it would have been very easy. We would have said make sure that their password is not Password, buy a SonicWall box or something similar to drop on your Internet gateway and install Norton or some anti-virus on all your laptops, and desktop and servers and you're done. That's pretty much all you need to do. And I know I'm vastly oversimplifying.

Today, 20 years later or 15 years later, everything has changed. An endpoint can be anything from - I see some Apple watches here, I've a Pebble watch, phones, tablets, virtual machines in the cloud, virtual machines in the data centre, virtual machines going back and forth. In a hybrid world, we have just about anything. At my house I have Nest thermostats. I never would have thought that part of my home infrastructure

would be an endpoint that needs protecting. So I've heard this $4 billon number with WannaCry; I've no way of really verifying it, but $4 billion worth of economic damage due to just one, admittedly large, malware attack.

The endpoint, as we all know, is under tremendous assault by all sorts of things, some of which are made worse by the end user or the IT person in a company not doing a particularly good job with security, some of which are totally beyond the control of the endpoint administrator or the consumer. You know, if there's flaws in the Android platform on your phone, there's very little that you as the consumer can do about it. Maybe even little that the carrier can do about it. So endpoints are under constant attack, between port scanners. It's the equivalent of people walking through a parking lot and just trying every door handle on every car to see which ones are unlocked. And maybe they are unlocked and they can steal your cassettes, if you still have some, or maybe you left the key in it and they can steal your car, or maybe they know how to get the car working, but they're off and going.

Terrorism we talked about at this morning's opening session; most of them that we're going to be dealing with I'm talking about here in this session, or we'll be talking about I hope, would be more criminals rather than state-sponsored terrorists. It's kind of like, I have a nice car. If someone is truly targeting my car, I know that they will be able to steal it. But if they're just looking to steal a car, I can do things to try to make sure that they steal someone else's and not steal mine.

So endpoint not that long ago were those end-user devices. We weren't as - we weren't talking about Internet of Things, or we weren't talking about wearables, we weren't talking about embedded medical devices and all those things quite as much. Maybe we had people setting up skimmers on credit card readers three or four years ago, but certainly we weren't hearing about them as much as we are now where it seems like every week there's another theft of someone stealing directly from the point of sale device. So that traditional focus on desktops, laptops and servers is no longer anywhere near sufficient when we talk about endpoint security.

So nowadays it's all those things; network infrastructure, SDN can introduce new vulnerabilities as well as new capabilities. In the more programmable devices you have, let's say the programmable Internet, any place you have programmability, you have APIs, you have SDKs, you have the opportunity to use them in ways that are not expected. There is something called the OWASP study which looks at vulnerabilities programmed into software. And the list of vulnerabilities that you see today in software being written today are the same ones we saw ten years ago: buffer overflows and SQL Injection and just bad coding practices. And we really haven't learned. And, of course, as we talked about in an earlier session, there's no type of certification, there's no government or industry certification that proves or demonstrates that most software has gone through a rigorous design and coding and testing cycle to make sure that it will be secure.

Protection is necessary, as we know. And as we also heard earlier today, once the bad actor has some type of foothold on a network or on a device, what they can do is pretty unlimited. So the goal of endpoint security will be to, first of all, try to deny them that

type of access; second, if they do gain that sort of access to be able to detect it rapidly; and then, third, do some type of countermeasure rapidly. Otherwise, again, once it spreads, as I think Greg Fitzgerald said earlier, it's game over - someone said that earlier. And we don't want that to happen.

One of the things I'm going to talk about before turning things over to the panel is a new term which I have trouble pronouncing, SysSecOps - try that ten times fast when you're still jet lagged - and it brings up the notion that, in many organisations, security and IT operations might as well be in two different organisations. And often they are; even when they report up to a common person, they're still governed as if they're two separate silos.

Scott Raynovich, who some of you know in his new organisation Futuriom, will be releasing tomorrow a study called Endpoint Security and SysSecOps. And it highlighted - I believe you will all be getting that study tomorrow - it highlights the gap between operations and security. As part of his research, Scott interviewed 140-odd organisations and they discussed that their top challenge is better - is first of all, lack of time and resources to really devote to endpoint security.

What they said they needed was better management and resources to merge operations across silos, and silos being operations, whose job it is to say yes. You want to do something to help the line-of-business manager, vs operations which says, heck no, that's not safe. I'm not going to allow you remote access to that resource even though you say it will help you do your job because my job is to minimise risk, not to create opportunity. Whereas the IT department's job is mainly to create opportunity. And they certainly want to minimise risk, but that's not job number one for them. They want to say, yes, and security, unfortunately often wants to say no.

What also came out of Scott's study, is that examining real-world breaches in these organisations, in these 140-odd organisations, revealed that they have tremendous gaps between organisational response. When the security team found out about a breach that was in progress, they often had no way to rapidly respond, other than perhaps they had some things or some levers under their control. But otherwise they had to rely upon ops and they had to figure how to transfer that knowledge to the ops team, so the ops team could then patch devices or revoke user privileges or whatever it might be. Or converse, that the operations team was the first to discover that there was a breach or something going on; they had trouble interfacing with the security team. They had different tools, different processes, different methodologies and often didn't even know how to talk to each other.

It reminds me, by analogy, of, in many large cities, the police and fire brigades have different radios on different frequencies. And so they find it very difficult to communicate and coordinate responses that require - the fire chief can't ask a policeman can you block that street so I can run a hose there? They have to go through layers of management and despatches. So too often these IT people - sorry, the respondents on Scott's survey said, things are not integrated across silos. And thus what Scott is calling for is that SysSecOps - did I get it right this time - SysSecOps need, which is not only have them speak the same language, but have them also share, in some cases, the same

tools and the same techniques, so that they can - they have the same data at their fingertips. They might use that data differently; the operations team might be applying patches, or teaching end users not to click on phishing emails, but they need the same data the security team has been gathering to say, heavens, we have a vulnerability. This is a zero day. We have to do something; we have some users that need some training.

So conflicting goals of security and operations and different tools and techniques, those are seen as the critical issue for our industry. And what Scott points to again, you'll see the study tomorrow, is a need for executive level integration in strategy, not only in the tools and techniques but also in setting goals and saying, you guys have to work together. You can't have one team whose job it is to say yes and one whose job it is to say no, but you actually have to work together and have - tear down that silo. That doesn't mean IT people become security people or vice versa, but they can't be on two different teams as much as they have been in the past.

And with that introduction let's go to our panel. So I would like to ask each of you to quickly introduce yourself and then I'll throw out the first question. We'll start with Steve.

Steve Broadhead

Steve Broadhead, Broadband Testing and also co-founder of the original NSS Group which became NSS Labs.

Roark Pollock

I'm Roark Pollock. I run marketing and product marketing for Ziften.

Carl Gottlieb

Carl Gottlieb, owner of Cognition. We're a consultancy company but also owner of testmyav.com.

Alan Zeichick

Right. Thank you and welcome again to the panel. So I would like to start by asking what may seem a fundamental question. Endpoint security, at what point do I need to secure the endpoint? Do I secure the endpoint at the endpoint itself by installing some software there? Do I secure the endpoint by securing what it's connected to? Or do I secure the endpoint by securing the communication path or by something different? Steve.

Steve Broadhead

At the moment it's all those things, isn't it? So we had a panel debate back in November in Dublin with Carl here, and Jason who is in the audience. And one of the things I talked about then was there's such a multitude of new security solutions, applications that are all talking about where they actually sit. And all of them seem to agree to disagree in terms of what is actually required where/when. So you're in a situation where, if you're an IT manager, security manager, there is no obvious answer to that

question at all, because you talk to ten different vendors, you'll get ten different solutions. And all of them will basically accept the fact that they are probably only part of the whole story, right? So...

Alan Zeichick

Everything.

Steve Broadhead

Everything, yes.

Alan Zeichick

Roark?

Roark Pollock

Yes. I think the answer is it's all of those. But I think what's critical is one of the reasons endpoint security has become so important and such a topic that people are talking about is because in the past, IT owned and controlled the endpoint and so they could manage that endpoint completely. And it was an easier problem to solve. Now they've completely turned the endpoint over to the business user. Whether it's a server or whether it's a client device, you have admin rights to the devices you have. You can install whatever you want on to it. And so it's a very difficult problem now for IT to solve.

What they haven't turned over to the business user is the accountability for maintaining security on those devices. And so now they still have to be able to maintain security on that device, even though they don't have the control of those devices. All of those devices, they're in hotels, they're working in hotels, you're installing whatever application you want on those devices. Or they've given over the server infrastructure to the business user so that marketing can run whatever applications they want to in the cloud or any place else that they feel fits their business models. So it's become a much more complex solution for them to try to solve.

Alan Zeichick

Carl?

Carl Gottlieb

So I'm going to take a slight contrarian view on this, that we as an industry look for perfect. All the time we say, what is the perfect place, what is the risk assessment on everything and aim for the perfect solution. And the problem is we get so obsessed with perfect that we never end up doing the basics, or even doing the basics right. So if we go back to, let's say, a small business, let's say an accountant, and say are you going to protect the endpoint, you can protect your sales force, protect your SaaS applications. They're just going to say, I don't know what you mean Carl, but I've got €100, what am I going to spend it on? And he's not wrong. He's not wrong. And the problem is we, as

an industry, are often quite arrogant because we'll look at that and go, well no, you're wrong, because you need to spend another £1000 here, another €10,000 there. You need to buy this solution, that solution. So yes, I don't care; I've got a business to run. What do I do?

And so we have to do a very quick risk assessment. We all do risk assessments all the time; do I take the Tube? What's safe? Or what shall I do across the road? And so in that organisation they'll say, you know Carl, I've got one PC, how do I protect it? Shall I just update my McAfee for another year? And that's probably the right solution for them. So we have to, I suppose, get out of this bubble that we're in of thinking that there's a thousand different endpoints and we've got to worry about the car, the Apple watch, the phone, the PC and say, if for your organisation, whether you're NHS or an accountant or whoever, what are you trying to protect? What do you really care about and what are some good, small targets. What are some quick wins that you can get. And if it's just upgrading to Windows 8 this year, then great.

Alan Zeichick

Yes, I couldn't agree more on the basics. We believe that - one of the things we really believe is that good security is the top of the pyramid. And then, if you're going to secure endpoints, whether they're server based endpoints or client devices, it all starts with having good visibility of what's happening on that endpoint device. And that becomes the foundation of everything that both IT and the security organisations need to do. You start with good visibility, that allows the IT team to actually manage those devices. And in a lot of cases, even the ones that sit on-prem, on the network, they're still having struggles with managing those devices; by that I mean just basic risk management, managing the patch levels, making sure the operating systems are updated, making sure that those devices are compliant to whatever policies that they have in place. But if they can't do that basic risk management, to your point, the security team has no chance. So if the IT team's not working and not successfully managing the risk on those devices, the security teams, really, there's no chance that they can secure that environment acceptably. So it all starts with the basic foundation of visibility. And that gives the IT team what they really need to be successful. And then, once they're successful, the security team has a lot better chance at being successful as well.

Carl Gottlieb

So basically, it's responsibility versus tick box, right? So it's very easy for a security admin guy to just say, put that in, I've got this solution, I've ticked the box. If they don't actually know what their network consists of, everything from endpoints to applications, LAN/WAN/cloud, to which version of a browser they're using, which OS etcetera, and it goes on and on and on, unless you actually know that, you can't secure it. It really is that simple.

Alan Zeichick

Yes, but how can you know that? I'm going to push back on a couple of points; one is, 15 years ago it would have been Windows servers and Windows desktops and use Microsoft system centre and run some discovery and, boom, you know what you've got.

And nowadays you've got everything, again from Apple watches to containers on Amazon to virtual machines running somewhere in Hong Kong, because you need to have a local presence there. And, as we heard in one of the earlier sessions, the interesting stuff you own is outside of your perimeter. So how, practically, in this world, in 2017, can I, as an IT department, as a security department have a prayer of knowing all the things I need to be securing, because, in theory, I need to be worried about the security of my partner's computers, because they have some access into my system.

Carl Gottlieb

Not in theory, in practice.

Alan Zeichick

In practice. And so how is this even possible to have any idea and then to take action, when I may not even own many of those devices or may not even know that that partner exists.

Carl Gottlieb

It comes down to one word, sponsorship. And this is the key of every GDPR project going on globally at the moment, is people are going headfirst into it, trying to implement solutions. But there's no backing from an Exec Board, there's no understanding of how it really fits into the business. And we have this issue where you can, look, do an audit of an organisation and say we have ten SaaS apps, 1000 desktops here, something in Hong Kong but there's no budget to secure it or even know what's out there. And the reason there's no budget is because there's no proper sponsorship of IT or info sec as a role inside the business.

And, going back to my analogy earlier on, if I've got a single accountant with a budget of £5 a year, then he's not valuing IT, just like BA weren't valuing the role of IT in their organisation. Now if you get ones that really do, then they say, yes, budget isn't a problem, because the business gets it and they say, yes, we have the money to buy the right people, the right tools, the right systems. And they can, effectively, roll out projects and know exactly what they've got and how to secure it.

Alan Zeichick

But Carl - okay. Let's say, on that second type of company, how do I do this? Okay, you've give me a blank cheque. How do I know all these things?

Carl Gottlieb

Well first of all, just a quick one, let's just drop this view that we have in an end user world that every tool is rubbish, that technology doesn't exist and there's nothing we can do about it. I can give you a great example; anti-virus. The security community of end users has written off anti-virus; it doesn't work, it can't protect me. And the only way to fix it is to look at other layers of technology; whether it be patching, whether it be EDR or whatever, anti-virus just can't work, can it? Now we know in the vendor world, that's wrong. There's new products coming out. In the endpoint detection and

response space there's great technology that's come out. We are in a really fantastic place. But unfortunately, so many people have given up because we've failed to deliver decent technology in the past, that we have to be optimistic sceptics and embrace vendors like these guys, and say, show us what you've got, can you solve our problem, and they can, and you embrace what they have to say.

Roark Pollock

Yes. I was going to say you absolutely can see everything that's out there today. One of the things that we do is we deploy on all of the endpoints that you want to manage and give you a complete view of what's happening on all those endpoints. But beyond that, once we're on that network and we see all the connectivity on that network, we can see everything that's connected to that network; every IP watch, every thermostat that you might have connected in the office. If you bring in a moisture detector for the ivy you have growing in your office and it connects to the Wi-Fi network, you can see all those things that are on the network. And we harvest all that data off.

So we're giving you a complete view, not only right now, but what's happened over the last 12 months in that network and on those endpoints so that you - it's effectively like having a hi-def video surveillance camera, watching all of your endpoints constantly, as opposed to using the Polaroid camera, which is what a lot of the tools do today. They take a quick snapshot, maybe once every one or two hours, and give you a picture of what's happening. Even though that picture develops in 15 seconds, you still miss an hour or two hours' worth of activity. And it's absolutely possible to maintain a 100% view of what's happening on those endpoints today.

Steve Broadhead

Yes. I mean, I've actually, like every aspect of IT, network management, in its broadest sense, has moved on massively. And I've tested various incarnations over the last 25 years or even more in fact, 27 years. And it is in a very different place to what it was before. They've had to re-invent it because IT has been re-invented. So on the one hand, yes, absolutely, and maybe a combination of tools. But the second element which is back to basics, has IT simply become far too complicated? The answer is yes, absolutely. Just end of story, right?

Alan Zeichick

So I'm going to resist the temptation, Roark. You mentioned ivy; I'm going to resist the temptation to do a Banyan Vines joke. So what about the role of carriers and telcos and so on? At some point along the line, if the endpoint is outside of your enterprise perimeter, it's connecting via an ISP or a cellular network, are there opportunities or responsibilities on their part to help assist in this? Or are they just dumb conduits and it's up to you, at the enterprise, to get whether it's an agent from Ziften or something, that you just have to do it yourself. And you can't trust WAN providers to be your partners and in securing endpoints, or can they be?

Roark Pollock

I don't think of the carriers, the telco carriers or the WAN providers, necessarily as being endpoint security solutions providers. What I do think is any of the providers that are out there that are providing managed services or managed security services, they're in a perfect place to help solve some of those problems. I think what Scott was talking about when he talks about SysSecOps, is how do I bring the basics of managing an endpoint together with how do I secure that endpoint? Well, the managed security service providers can do all of that for a lot of these smaller customers, or even larger customers, where they're outsourcing the entire responsibility of maintaining visibility and control over those endpoints and being able to secure those no matter where they go. Whether it's on the customer's network, whether it's working remotely from a hotel like this, or even if I'm just connected completely, they're in a position where they can start to maintain security on those endpoints no matter what.

Steve Broadhead

Responsibility is a key factor here so, it's only really in IT that you actually spend potentially billions of pounds/dollars on technology. And it comes with absolutely no guarantees whatsoever right? If you buy a washing machine, you get a three-year warranty. If it breaks, you get it replaced, right? And it's still a world of finger pointing. So a service provider will try and shy away from - they may go for a performance, your SLA type of thing. But on a security level, there is absolutely no guarantees that one party will actually say, yes, we'll hold our hands up, that was our problem, or even share what's going on at that level. So if you're a company, you outsource, cloud whatever, you don't actually know what they're doing really to secure your data and applications. And they don't openly tell you, do they? So, you know.

Alan Zeichick

So before we open to questions, one quick, final question from me. I was talking a bit; I was sharing Scott's data about SysSecOps, would you agree that the silos between IT and security have been an impediment to having more streamlined response to incidents and better security, or do you think that really things are going fine. Security should do security, ops should do ops and they can meet in the lunch room when they need to.

Carl Gottlieb

Yes. I think, I suppose the answer is fairly obvious that everyone needs to work together a lot better, but it's still their fault. They're not - it's dead easy to just go and talk to people; it's not rocket science. And these are like hey today I'm an IT guy, tomorrow I'm a security guy. The world hasn't changed. We've all got responsibility, whether it be the business tying us together. I was at an HR conference last week and saying it's HR's responsibility to represent these different departments and bind them together. We all have different focus; dev to dev, IT to IT, sec to sec. It's just the way it's going to be until we actually work together a bit closer.

Roark Pollock

Yes. I think we all make the assumption that everybody within the organisation is working together to help solve a lot of these security issues. But the reality is it just isn't true. In a lot of cases the security team and the folks that are responsible on the IT team for managing risk, they don't even know each other. They don't even know who they are, they don't know where the other person sits. And so there's no way they're working together in a coordinated fashion. I hear it from customers all the time. If I'm talking to the IT guys, they don't know who is on the security side or vice versa. And so it makes it very difficult for them to work together in a coordinated fashion. Once something happens and they have an incident they need to respond to, they have no chance.

Steve Broadhead

Yes. Just to make the point, there's nothing new here. When I started in IT it was data comms versus tele comms right? And the two generally tended to loathe each other, right, so they really wouldn't even go to the same meetings. And it's the same now. And the kind of resource allocation is the issue as well where you've got different levels of technical ability between IT and security and, and, and. So they don't actually - even if they do talk to each other, they probably don't understand each other.

Audience Q&A

Alan Zeichick

And so speaking of understanding, now is the time for us to understand your questions, and so, Jan.

Jan Guldentops, BA Test Labs

I've got a couple of points. First of all, what bothers me a little about the endpoint is that we're going for one solution fits all, right? We're throwing everything on a big heap and try to secure it the same way. And that's not going to happen. In the end, the consumer updates of my Fitbit would be the responsibility of Fitbit; it will never be the responsibility of the end user, because he won't be able to do it. So it's - I think we need to separate there a little; the first point.

Second point, Banyan Vines? It's ten years since I heard that.

Alan Zeichick

Well you know, the old jokes are the best jokes. They're classic.

Jan Guldentops

And last but not least, have we finally got rid of the perimeter or are we still thinking that way, with isolation and VLANs etc., or are we just going to get rid of that completely?

Alan Zeichick

So first of all, I think I take issue a little bit today is that the application providers may be responsible for providing the patching, but users, the best thing you can do to protect yourself today on any endpoint device is just keep your applications in your operating system patched. Hit that update button every day, every week and make sure your applications stay patched. You don't want to be in a position where your iPhone or your device says you have 450 patches that you need to apply that you haven't done in the last 12 months. That's what caused the WannaCry worm. All you had to do was patch your systems and you weren't exposed to that particular issue, and the patch had been out there for a long time

Steve Broadhead

But that goes back to the basics of just human error, doesn't it and maintenance and it's nothing to do with technology. The technology is there, absolutely, but it still has to be used correctly.

Alan Zeichick

Well I think also a lot of false positives. You get hundreds and hundreds of patches coming out all the time; limited IT staff, which ones do they do first?

Jan Guldentops

All of them.

Alan Zeichick

All of them, well, in a perfect world.

Steve Broadhead

But also, Jan, on the point of endpoint isn't an endpoint, absolutely agree. Would you secure a smart watch in the same way you'd secure a data centre, but technically you could call them all endpoints. Absolutely not.

Jan Guldentops

Because a lot of those devices are not capable running security. You can't do encryption.

Steve Broadhead

Right.

Jan Guldentops

It's not feasible at this point.

Steve Broadhead

Correct, absolutely.

Carl Gottlieb

And yet, as a security threat, that endpoint is probably more vulnerable than, you know...

Alan Zeichick

Especially if the admin manual can't be changed, and it's password it's written in the manual. So I think - do we have time for more or we don't? No, we are done. Thank you very much. Thank you panel.

Manek Dubash

Thank you Alan and thanks very much to the panel. And now we move on to our last panel before lunch, talking about practical application…

[end]