**RedZone Podcast Episode #99: Block First, Ask Questions Later | Security + Business Continuity with Dmitriy Ayrapetov, Execuive Director of Product Management at SonicWall**

Bill M: 00:00 Well, we are live. Dmitriy, welcome to the show today.

Dmitriy: 00:04 Thank you for having me.

Bill M: 00:07 I am certainly going to have a little intro for everybody that will have covered who you are, but why don't we just, from your perspective, just so everybody knows who you are. Talk a little bit about what your current role is at SonicWall and how you got started in this industry.

Dmitriy: 00:26 Sure. So currently I'm executive director of product management at SonicWall in charge of network security. Everything that relates to network security, and we are a security company, falls under my view in product management. I got started, I actually have to say this, almost exactly 20 years ago, and kind of by accident. I'll tell you a funny story, and it's the little things sometimes that really set you on a different path, right? I was in the dorms in college and people are passing around different software and there was one little program called wack-a-mole, it was little game, but really under the surface ... I think you might know where this is going. Under the surface, it was actually a full on remote kind of administration. I'm not going to say on your podcast the exact name of the software was, it's not exactly clean, but it was a full remote administration software.

So I sent ... And I was at Berkeley, and I sent it to a friend of mine at Stanford, one of my best friends, and it has nothing to do with the Berkeley-Stanford rivalry. For those of you on the east coast, big rivalry. But I sent him this program and I said, "Hey, check it out." He clicked on it and he said, "Okay this for kids, why are you sending this to me?" So, I'm talking to him on the phone but now I have actually access to his computer. As we're talking, I'm putting up dialogue boxes on his computer that are relevant to our conversations on the phone. Imagine, you're talking to me on the phone and your computer's popping up dialogue boxes that are like, don't say that, I warned you not to say that. I start hearing this pause in his voice and this nervousness in his voice, and he's like, "Wait, something really weird is happening." He was a really good friend of mine, I don't have that much of a mean streak in me, I immediately told him what I was doing and I deleted it, we cleaned it up.

From then on, I kind of just like tracking, you start reading about this, then I came across, again, sort of by accident, across Hacking Exposed. Many of you might have read that book, I think we're on volume five or six now. It was like Hacking Exposed Volume 1 or Volume 2. I read it, and it was interesting, and I was like, "Wow, this is really cool," and just one thing leads to another. I never thought I would go into the security industry and then I work in one start up, I worked in another start up, that start up gets purchased by SonicWall, next thing you know, I'm talking firewalls, I'm talking malware, ransomware, all that stuff, but the spark started 20 years ago with that little prank.

Bill M: 03:02 Wow, that's great. That was probably in the late 90's was it? Middle 90's?

Dmitriy: 03:10 Late 90's. The wild, wild west of the internet.

Bill M: 03:13 Yeah that was a crazy time then when a lot of stuff was coming online, and the real internet was probably just launching in 95 as far as from a browser perspective.

Dmitriy: 03:22 Yeah. Yeah. This is one of those ... And I've been online since earlier, my parents, my father especially, had a lot of foresight about, what's kind of coming up and when we immigrated here, he got me a computer, he got me on NETCOM. I don't know if any of you remember NETCOM? Yeah. I learned, by the way as an aside, I learned the lesson of the permanence of the internet very, very early, because when Google purchased Hughes Net, remember when Google purchased Hughes Net? I started searching, and I found conversations of the 14 year old self, arguing about whether MiG-29 is better than F-16 and one has laser aimed-cannon. It was just silly, right? But I'm like, "Wow, this is now forever archived on the internet." So if you know what to search for, and I'm not going to tell you the terms. So that was early days but also early lessons.

Bill M: 04:18 Now, you immigrated from ... Where did you immigrate from?

Dmitriy: 04:21 When we left it was actually still Soviet Union, but the actual republic was called Moldova. It's an independent country now, but it's one of the republics. Yeah, but when we left it was still Soviet Union, as you can maybe tell by my accent.

Bill M: 04:34 Just a little bit, and it's always interesting to see where people have come from because that's ... Land of opportunity, and I sometimes think people immigrate and have somewhat of an advantage, just the multi generations that maybe get started afterwards.

Dmitriy: 04:52 Yeah, but I will give a lot of credit to, especially again, my father in that he basically, and maybe that was his way of keeping me out of trouble. He just got me a computer and got me an internet account, he was like here [inaudible 00:05:04].

Bill M: 05:04 Go figure it out.

Dmitriy: 05:06 Yeah, go figure it out, have fun.

Bill M: 05:08 That's great. I was really ... My CTO, I think as I mentioned before, he has very few guys that he really looks up to, and you're one of them. He's talked to you repeatedly and he's just really encouraged me from probably about a year now, to have you on the show. I want people to get an appreciation of the landscape that you're navigating from a threat perspective and then I want people to understand about SonicWall as well. And I think one of the pieces we can start at, is what do you spend most of your time thinking about these days regarding solving problems?

Dmitriy: 05:58 That's a really good question. Let me answer it like this, there are multiple layers in how I think. My casual reading in the evenings is, I have my social media forums or accounts that I follow and that I read, and I try to absorb a lot of information of what's going on. And a lot of it is, some of it is blog spam, right, some of it is just rehashing of or regurgitating of what's already been written, but some of it is truly novel. What really gives me a picture of reading a lot of that stuff, is kind of the side guy, so the temperature of various topics, and you can see what's trending, what's like really, really early on, what's about to peak.

When I think about the, you asked me how do I think about the landscape? I treat it in two different spheres. There's one sphere which is almost like personal enrichment and personal education, and I think we all have to do that and whatever our domains of interest or professional domains are, it's like what's the state of the art? What's going on in the industry?

Forget the company I'm working for, or forget what we're doing. What is really going on? Right? That's the first sphere of it, the kind of sphere thinking. And then the second one, of course, is okay, how do we apply that to what we're doing within the, kind of what I call the maneuverability envelope of the organization that you're in?

There are those two angles. On the what are we doing about it right? That translates into what do I put on the roadmap as an MRD from a security perspective. Like for example, three years ago, it was actually three or four years ago. Ransomware. It was a little blip here, it was a little blip there. You start reading forums, people are freaking out, asking questions, you start asking yourself, "Wait is this a new thing?" Then you start thinking about, "What would happen if this happened to me?" Then you realize, "Wow, this is actually really, really dangerous," cause it's going after the most valuable asset, which is data.

Forget my laptop I can lose my laptop I'll replace it. Yes there's going to be a financial cost, but you know what, I'll eat it. But the data on my laptop look at it at home. Like, somebody's pictures at home, their family pictures. That's the real value. You see this one instance, you think, "Wow. How impactful is that?" And you realize, that's very impactful. And right away we're like, "Alright." And then I switch my hat into, "Alright, I'm a product manager for a company that actually is directly related to this. What do we do about this guys? With marketing? How do we talk about it? How do we educate, engineering, how do we block this? Blah, blah, blah, et cetera. I'm not sure if I'm actually answering the question. I'm more like ruminating of like, how do I explore topics? Again, there are those that are like, "What affects the company directly and what affects our customers."

But to me that's a byproduct of personal education and personal looking at what really happ ... What is security, what is happening, what are the trends, what's going to be happening five years from now? And I put myself always in my mental process for this is I imagine that how would I personally react if this happened to me, would I shrug it off or would I move on or if I was a startup founder with, whatever, $100,000,000 of VC funding, would I pursue this problem or how would I pursue this problem? Right. And those are useful kind of ways to think about the issues.

Bill M: 09:34 Actually, that's really good because I was thinking when I was putting some questions together. How you view the world because you're, having to see around the corner a bit, not a bit. I mean you really are trying to map out and almost like have subtle heartbeats into what's happening and what ... And so you can navigate the company's product set to meet that need down in the future.

Dmitriy: 09:59 Yeah.

Bill M: 10:00 And you've been doing this for so long now that must be somewhat of an instinct, but sometimes I was curious, is there, you've already answered some of the questions. You're going to a lot of social media, blogs, forums, places that you go to kind of measure the heartbeat of where we are, but then you also had a great question that you asked yourself. If you're a startup founder, what problem would you be out there to solve?

Dmitriy: 10:21 Yeah. I'll give you, just let me even make it more concrete. Fundamental job of product manager can be summarized in, you find people's problems and you bring those problems to engineering. If you just do those fundamentals, just find the problem and don't listen for feature requests, feature requests or people's versions of what they think the solution to the problem is. The real job of a product manager, kind of a philosophical level is find problems and bring them to, and with engineering, bring solutions to the market to those problems. Right? And a lot of those social media and the forums are not even necessarily about cutting edge security or anything else like that. I read networking, I read CIS admin forums and i look at what questions are people asking each other, right? Because when you see very popular threads on people asking each other certain questions and they have a security bed, that's a problem.

That means people are having a problem. They don't know how to solve it. They're turning to their peers. And if there's a lot of debate or discussion around it, that means there is no consensus on what the solution to that problem is. So that might be a fertile area of exploration of, and maybe, and again, if it's security related, hey, maybe there's a new trend, right? Maybe there's something happening there that we're not paying attention to, but you start getting real people with real day to day jobs. Articulating that as being a personal problem.

Bill M: 11:43 It's fantastic. It was interesting, in 2007 we started a, this was well before 2007, but right around that time we were strong, at that time they didn't have managed services as of ours. Strong bar for the SonicWall firewall. And you guys had released this firewall that was just, it leapfrogged the competition. And then all of a sudden the economy crashed.

Dmitriy: 12:10 That's right around the time when I joined product management. No court, no causation, just correlation. That's right. I know exactly what you're talking about.

Bill M: 12:18 And then all of a sudden all the R&D funding from a lot of the major firewall vendors evaporated. And it was like there was SonicWall, with this really advanced capability. And then there was this white space of time because the economy was, a lot of R&D funding had dried up and then in 10 years, now moving forward, we are at a different stage, but you still have some of those older product sets. And I'm curious, where do you see some of the newer capabilities that you liked to talk about today from a product management perspective? As far as meeting really important needs right now?

Dmitriy: 13:03 Sure. let me think.

Bill M: 13:07 I can preempt this a little bit because I ... Let me preempt that so I give you some time to think because I think it's important. I look at the human immune system is like this ... We have this automated response to, within the human body and a normal functioning human body to respond to infections and cuts and bruises and sort of, the body deploys automatically. And I look at the market and I look at where we are from a security threat management and how do we create this immune system response with products like we do in the human body and is there even a possibility of doing that in the future.

And I look at like the ability for a person, a human being to click on something and yes we're raised trying super hard to educate them and train their users, but the reality is they're clicking stuff they shouldn't be clicking and then that's infecting, that's causing an infection of some way, shape or form. And I'm loving to see how you guys look at that from a world perspective and how you've mapped that too from products and, and where you see things are happening now with that.

Dmitriy: 14:12 Well, thank you for clarifying that's a perfect question. And just knowing who a lot of our customers are and a lot of our customers are the small, medium businesses, small, medium enterprise. And a lot of them just need automation what's now called, security automation. Don't tell me that 15 minutes ago I got ransomware. That doesn't help me, the damage is done, block it from me. And so I'll give you some concrete examples of what we've done. So for example, when we launched our Sandboxing service our cloud sandbox analysis service called capture, what the state of the art in the industry at the time was, it was files, attachments, downloads. They get sent passively, kind of on the side. They get sent into Sandboxing and 15 minutes later some admin or some system or some sim in the network gets an alert, "hey, Dmitriy downloaded an infected document, good luck." Right?

And that was the downfall of Target. That was the flaw in the Target breach in 2014 or so. We saw that that was the state of the art and we were launching. And we said, "Well, wait a minute, that's not what a lot of our customers want." Our customers want. "Hey, did you take care of the problem for me? Don't tell me that there is a problem. Did you take care of it?" So we introduced something called Block Until Verdict. Our Sandboxing solution actually, the way they operated was it sent the file to Sandboxing analysis, but it didn't actually let the user get the entire file. If you're downloading a program or a word document, you actually can't open it until we let you open it, until we give you the right. We were holding some of the data back and like, "Oh the download is a little slower, just wait a little." While in the background we're actually testing it. And if during that time, during that period that were making you wait and it's a little bit of an inconvenience, but you know you have to do this, you wait.

And if during that time we find out that, that was actually infected with malware, we actually cut off the download. We don't let you get the rest of the file and therefore your computer doesn't even know how to open it because it's corrupted. You can almost think of it as like we truncated and the users are just like, "Oh, the file doesn't open." And then we put up an alert that says, "Yeah, you're downloading ransomware." But the end result is that we automate that security. You can even see that on the client side. So when we, a year and a half later when we launched our kind of next gen behavioral analytics, behavior analysis based antivirus client, there is the concept of remediation, rollback. People don't want to be told, "Hey, you had a problem." They're like, "Yeah, what'd you do about it? Did you solve it for me? What are you going to do about it?" That's what people want to know. And so those are two specific examples that affected our product design or what we decided to launch. Yeah I don't know-
Bill M: 17:18 Yeah I love that. I'm so glad you started there because it's like block first ask questions later and people just don't have [inaudible 00:17:28] continual theme every time I'm talking to, it doesn't matter the size of the company could be the big companies, it's just very difficult to staff enough people and to be able to do this and people wonder, machine learning and AI's taking over jobs. Forget that. We need machine learning AI tools to be able to think intelligently about this needle in the haystack incident. So I love how you've taken the approach of coordinating off and Sandboxing and killing and all the way down to the client side. I think that's powerful, but you're also doing it, it initiates at the firewall, correct? You're doing it about the firewall [inaudible 00:18:10].

Dmitriy: 18:09 It initiates at the firewall. Absolutely. It all starts at the edge. That's why the firewalls sits in a very privileged location on the network. Everything goes in and out through it and yeah it all starts with the firewall. But can I take that? Can I think that whole idea outside of just even network security. Like I mean you have a broad audience and I want them to, I want to share like a way of thinking here. So one of the luminaries kind of in the network security world that I admire, that I follow, his name is Dan Geer and he is the CIO or philosopher and residents I don't know which title he uses at the company called In-Q-Tel which is really the VC arm of the CIA, right? So he does a lot of research and he's a fascinating character and one of his recent writings was, and I think this is a very useful way of thinking for everyone just outside of even security.

What about security? He said, "Look, all of the emphasis and security has been put into prevention, but there is not sufficient emphasis that you continuity." What if we made an analogy to power, like a power in the building. Imagine that power utilities put all their emphasis into prevention of a power outage, but non into continuity it would fail. What they've done instead is they said, "Look, we're going to spend a lot of time working on prevention, but we're also going to say that if the fault happens because faults do happen, sometimes things happen. We're going to get you back and running in under a minute, whatever under a second." Right? So from your perspective as a user, you're like, "Well yeah, something happened, but I don't care. I'm still operating." They're more critical systems. There's a millisecond fail over or whatever, but the point is it's about you assume that something will happen sooner or later.
You cannot operate in a world of 100 percent protection or 100 percent prevention of a power failure. But what do you do after that? Do you have a catastrophic failure at this point or do you say, and his idea was like, we need to get the security industry to the point where it's almost like power. It's almost like a utility. Yeah, there was a blip. It's okay, we're still running, we're going. Right? What's that post event technology that does it do remediation. Does it do automatic roll backs? Does it do, and this is where backups come in, but I think it's a very useful mindset. I love that analogy, right? It's a very useful mindset going outside of the firewalls, going outside of clients. It's your backups, right? You do backups, but again, then gears, [inaudible 00:20:35] are, have you tested your backups in a way where you know, somebody should be able to come in, pull out a 12 gauge and shoot any random piece of your equipment in the data center.

Are you okay? Do your backups work or do you have a critical failure? So that's one of the, again, this is like coming back to that earlier part of the conversation where I said there is like the philosophical and then how does it translate into actual product or design or anything else at that. This was the philosophical, the example that I found extremely powerful, right? Because it really translates into how you think about product design, how you think about your infrastructure design. Like are you designing, are you putting all your eggs in the basket of prevention, but if point zero one percent chance does happen, you're absolutely messed up. Or do you balance it out and you say, "Yeah, I will assume that something might happen." People make mistakes, but it's okay. We've got a backup plan.

Bill M: 21:27 Yeah, I love that.

Dmitriy: 21:28 Does that make sense?

Bill M: 21:28 No, it totally does. It's interesting. Now that you're talking about the parts of the reading you're doing, the philosophy, design principles. You're really looking at this from design, from a design philosophical principle like continuity of operations, like the old style-

Dmitriy: 21:46 That's it.

Bill M: 21:46 That disaster recovery was this three ring binders sitting on the damn shelf and now like security is DR. DR is security and you're absolutely correct. And so what you're saying is that, that's influenced your design, your actual product decisions because you're looking for how can I provide continuity of operations?

Dmitriy: 22:06 Exactly. And that's just because that's my world, that's my domain, right? I controlled or I work with engineering and we build roadmaps, etc. and I say, "Guys, okay, now for the last three years we've been putting a lot of effort into prevention, but hold on, do we have a gap here? Do we have a gap in remediation? What do the customers do?" I mean this is the conversation we have internally, but that's my domain, but the message that I'm trying to also carry again, like it goes outside, I want people just to be safe and secure. It's outside, even the firewall, it's when you're doing everything. When you're designing your system, like if you will have, whoever is listening to this podcast that the IT managers, CISO, CIO's. Do you have as you said that continuity of operation? And In my world, I control that through the firewall through whatever we do on the network security on the client but there's a bigger world also and I think this mentality, this way of thinking is extremely good in the security industry.
Bill M: 23:04 Yeah. I was just talking to the CIO, just before our conversation of Boston Scientific, I might be getting the name, it's something scientific, but they multi thousand user organization than they deal with gas sensors and handheld gas sensors and people can lose their lives and they have a ton of IOT, basically IOT devices around the world and he's spent a lot of time into building continuity of operations because it really impacts people's lives and so for them, these design principles are mapped down all the way to the end user impact in their customers. And then he's also an interesting piece as well, is that more and more sales people are coming to him starting in about three years ago. So they've actually had to turn that capability into a competitive advantage so they don't add latency to their sales process. So they can quickly get the customers that want to buy from them and subscribe to their services. They can get really strong answers to their continuity of operations that may affect them if they have a takedown.

Dmitriy: 24:11 Yeah, That's perfect, right? And the threat of security risk has really become front and center over the last six or seven years and I think it's really, unfortunately it was negative events that brought this into the commons fear of thinking is, 10 years ago security was still kind of in most companies, security was the operation that's running out of the closet, right? And it's the events and for the unfortunate events of the last seven years, all the breaches, et Cetera, that brought it to straight forward where now companies think about their operations from the concept of like, "Well, what happens if we have a security breach?" And in a way this also connects, I told you that story of how I got started in network security, but there is an arc of what happened to the network security field over those 20 years.

So I started out with that little prank on one of my friends and that's exactly what it was at the time. That's exactly what security was back then. It was people. And by the way, what I was doing, let's just be clear, I was a script kitty. The industry term for somebody who just download somebody else's software and pushes buttons, right? They don't know what really what's happening, but they didn't write it, so I fully admit it, but the point is most of the, even hacking defacement, et Cetera, it was all just people pranking and showing off to their friends. It was for Internet points effectively. Then in the two thousands, in the knots or two thousands, whatever we call them, it started turning more towards commercial operation, This started being like, Okay, I can make money from ... But it was more about stealing credit card information.
It was all about carding, but it started going more underground. And really it was the late two thousands and the early 2010s where it started becoming, alright, this is organized crime, this is real business, this is real money, this ROI in this, nation states started getting really into that. So it's evolved for pranks to just simple threats. I mean simple attacks such as just caught stealing credit card numbers to now it's front and center and it's, boardrooms consider what's the implication of a security event on our business operations.

Bill M: 26:26 Are you finding that, what's really been interesting for us recently in the past six months is the amount of credit card, no not credit card. A wire transfer fraud, that's happening and we've had engagements with people from anywhere from like $750,000 loss to as low as 10 and, but it's very, very patient but it's very targeted. It's not like a brute force, but it's very certain. But that's happening right now. Do you see that expanding or do you see anything else that will build upon that moving forward?

Dmitriy: 27:08 The thing that, I think that's a specific instance of a type of an attack. I'll tell you what moving forward, what worries me. I'll tell you what keeps me up at night right now. I don't know if they're actually good technical solutions yet to this, but things like supply chain attacks, so supply chain, if you know what happened in Ukraine last year with the ... That's how WannaCry broke out, the multiple instances of this where common software commonly used software, the software vendor itself gets compromised and then their update servers are compromised and they through trusted channels. So your, whatever. In Ukraine it happened to be the accounting software. So imagine you're QuickBooks downloads an update, but the QuickBooks update server was compromised and now it's distributing, a spying software, ransomware, and there's nothing that you're not downloading anything that's overtly bad.
And it's coming through encrypted channels. That's one of the emerging areas. And I think only nation states so far have been exploiting that. I haven't seen a commercial hackers go after that yet, although I, it's another area where I had personal experience back in 2007, but it was completely by accident. That's one of the areas that's expanding, but really will come down to people will go where the money is, where the easy money is, malware is now run as a business. They're literally looking at the ROI whether they know it or not. They invest money into hacks or exploits. Exploits are expensive. They even carry monetary value on the market, right? But you spent six months. Let's say you hire 10 programmers, they clank away the keyboards, they find an exploit. If you. Now how do you monetize that exploit? You want to be very, very careful about how you do this, if you do this with very, very in your face malware, it might get detected and it will get shut down very quickly and you don't have your ROI.

So there is an incentive from the attacker's. You mentioned the word patient, right? They are getting more patient because they know that, listen, I cannot get detected right away. I have to do this carefully. I cannot be reckless. I have to just, in order for me to recoup my investment. And then once it gets discovered and it gets hashed by everybody and by the enterprise, don't forget, then there is the entire consumer market which is behind, which doesn't patch, that's when the malware just drops in value and that's when you get these mass, whether it's waterhole attacks, whether it's phishing attacks, where they're just looking for the people who like, an organization like an enterprise or even an SMB that's protected by any of the Next Gen firewalls. They won't be affected by this because they got it. They already know how to block it. What about you at home, not you per se you probably have a good firewall at home, but what about your friends at home, then that becomes their next target. So there is almost like it goes down in the value chain of attack. Does that make sense?

Bill M: 30:07 Yes. That's what you see as, your calling that like a supply chain, that's one of the things you don't think there's necessarily a solution out, but it's something that you see one of the problems has to be solved.

Dmitriy: 30:22 Yeah. The supply chain attacks have to be solved. That's where the update service get compromised. The other part is more like, the other part that I was mentioning where the malware, once the high value malware eventually makes it out to mass market, I think that's just where even consumer products have to get better at security. But now I'm just on a soapbox.

Bill M: 30:44 I want to also dispel, what's really interesting is there's this big push about year and a half, two years ago to start the marketing departments. We're really talking about machine learning and AI and it was just, makes me wanna throw up because I was going out to RSA and everybody, everyone has an AI this and everybody has a machine learning this. No one knew what they were talking about. And then it's funny that it's quietly subsided, it's not as much marketed anymore, but I'm wondering from some of the tools and such that you guys are looking at from a runtime detection, RTDMI, and some of the advanced threat protection we're looking at, where are you seeing and what's real AI and what's real machine learning in a security environment from your perspective?

Dmitriy: 31:33 Great question. Machine learning is a very, very good, and you're right, there was a lot of hype and there might still be a lot of hype, but it's a very, very useful tool. And what it helps you do is it helps you augment your human capabilities with machines, but in a smart way. And machine learning doesn't become effective until you have a lot of data because you have to, I mean there's a learning component. You have to train the algorithms, you have to train the neural net. All of that on real data. So this is actually in, I will toot our own horn a little bit here where through the virtue of how many customers we have at SonicWall we protect over a million networks worldwide, and we have email systems, we have a lot of very sophisticated data collection mechanisms and we get a lot of data with which we can train these systems. But let me just explain. I think people will find it actually really interesting of how AI helps in network security. I'll do it through kind of a simplified parable of antivirus, right?

Previously antivirus would just look for a hash. Okay. They're 10 billion hashes. You can't keep up with that. Now we start looking at, we can take a file, we can break it down into components, vectors and those components are, can be things like what's the file type, what's the file size, what's the entropy on the file? Does the file have calls into libraries that open network connections? Does the file have, try to open registry. There are all these different components and things that you can just observe about a file, whether it's an executable, whether it's an excel file, I don't care. You can extract these what are called vectors and you feed these vectors into machine learning algorithms and you train these machine learning algorithms by saying, when you see this combination of vectors, this is bad malware and you train, you say this, look at this one, that was good. Look at this one. That was bad. You do this millions and millions of times and then that's how you-

Bill M: 33:39 Can I ask you a quick question about that. So you have that vector. the file, you're looking at vectors within the file and then that feeds an algorithm which is essentially like a math program. Is that correct?

Dmitriy: 33:51 That's exactly it. They simplify what many people know is neural nets. There's a lot of statistics and math that goes behind it. And it's how you train, there is backpropagation algorithms. How do you train this thing to basically say, "Look, I'm going to give you ..." And these vectors you can also call them attributes just in machine learning they're called vectors and you say, "Look, I'm going to give you ..." We know how to extract these thousand vectors, a thousand attributes about every file that comes in, but what we've done first is we took our library of whatever samples of malware. We extracted the same vectors out of them and we trained our machine learning algorithm to, through with this library where we kept feeding these files and was saying, that was bad you saw that that was bad. And when the algorithm says, "Wait, but I thought that was good." And we say, "No but that was bad."

There are statistical, again, the backpropagation algorithms that go back and they adjust the weights they adjusts the values within this machine learning network and sooner or later you start reaching these accuracy levels and that's where machine learning really starts coming in. Where you say, "You know what? I don't even need to know the Hash of the file. What I'm going to do is I'm going to look at the file, I'm going to extract these vectors out of it. And I'm going to feed them into my algorithm and I don't need to update that algorithm every single day, I need to update it maybe once every quarter or something." But it can tell me based on the experience, quote unquote, whether this is a bad or a good file with a certain confidence level and then we set the threshold above what confidence level do we consider to be malicious.

And then this is the kind of a simplified essence of machine learning in the security industry. So like when we say in the RTDMI is a whole different beast. That's how we instrument the CPU instructions in the program in such a way that we see exactly what it's doing. And we can tell it if it's trying to evade detection by waiting for 12 hours, we can say nope, pretend the 12 hours have already passed we can rewrite the program [inaudible 00:35:51]. But that's where all the machine learning kind of really, really comes in.

Bill M: 35:55 Okay. We'll cover RTDMI in a second. I love the way you distinguish the [inaudible 00:36:04] because you had the machine learning piece which is a, you can say, "Hey listen, all of this data is going into the algorithm now based on experience I can make some assumptions." The machine learning is like, it's kind of a binary analysis, x equals y, but when you can make an inference is that where the AI comes into play when you're using multiple algorithms and then there's an overlay algorithm that kind of watches.

Dmitriy: 36:31 I want to correct. And again this is, we're not doing justice to machine. There are multiple kind of Venn diagrams here of machine learning, deep learning AI and the intersections are complex. It's very important to understand that machine learning is not like a bunch of if statements like if you see this, then plus one, if you see that, that's plus two whatever, plus two to the score. That's very rudimentary heuristic based from 20 years ago, for example, what this says is literally like if you look up like deep neural networks, multilayer neural networks, and there's a tremendous amount of mathematics and statistics that goes into this. And by the way, part of the reason why it's a professional interests, but it's also an academic interest because one of the things I was studying was cognitive science and computational modeling, but this is all where it's a lot more than just if statements and plus add the risk score plus. You have neural nets and they have weights.

They have statistical weights and you have inputs of these vectors that the algorithms run these vectors through the neural net. And you get an output score of let's say point nine eight. And you say, "You know what, things that are above the threshold of point nine six, we will count that as malicious." Now somebody might protest and say, "No, that was a good file." We would say, "Wait, why?" And that's where the humans come in. That's where they base sect it. Then they say, "Look." and they say, "Oh yes, this was a good. This was a remote team viewer program." I'm not saying anything bad about team viewer but just some program that might seem like it has behavior that might seem malicious but actually has a good purpose. Okay We'll make exclusion. But listen, it's behavior really was like most bad programs that we've seen do. And that's where, that is the machine learning, people toss around AI, deep learning, machine learning. It's a much more complex, let's just call it machine learning for the purposes of this conversation.

Bill M: 38:32 Sure, that matches to the continuity philosophy in the continuity of operations we were talking about. So what you're saying is you can create at the end point or at the firewall level or in the cloud, you can basically create these mathematical models, and then you can park these malicious potential misses files for detonation or for examination prior to enter into the network to cause damage. And is that where RTDMI and other tools pick up from there?

Dmitriy: 39:03 Yeah. So there are two elements. There's an element on the network where the file is being downloaded to get sent off into the capture cloud and that's where it undergoes this analysis. And this is when we talk about multi-engine approach, RTDMI is the engine that does all of this analysis, but RTDMI is also, there's also a memory specific algorithm, but then there's protection on the endpoint. There's stuff that's happening on the network in the cloud and the same thing, but with different implementation happening on the endpoint. And the reason why that is, is I mean when you're inside the network, it's an insurance policy, but really it's for when you leave the network, when you're outside, when you're in the cafe or when you're working from home, we want to say, you know what, we want the same type of an algorithm, we want the same type of protection for you to be on your end point. And now what we've actually done is we've plugged in, we've plugged in the point to when the endpoint point algorithm is not sure we're actually going to send that file to the cloud into the same thing that the firewall does basically.

Bill M: 39:03 I love that.

Dmitriy: 40:08 And we'll run it through the full gamut to like fully resolve this issue. It be like if the endpoint says it's point nine six, I'm not sure, we're going to say we're going to resolve this for you. For sure. And then we send-

Bill M: 40:17 This is what people have to understand this, I mean I don't mean to interrupt you, but this is so critical for our security moving forward because with the cloud, with a multi-cloud, with hybrid cloud, I mean people are all over the place. Nobody's moving. People thought they were going 100 percent of the cloud. It's not happening.

Dmitriy: 40:17 100 no.

Bill M: 40:30 It's like during these bridged worlds and then they have untethered users. And so I just love that [inaudible 00:40:38] that end point. The way you've done it, I think it's exactly where security needs to be.

Dmitriy: 40:44 Yeah, it's a critical. They're complimentary. Again, inside the network, let's call, let's say you'll protect me by the gateway, but you know, I'm on the road like 30 percent of the time, half the people are traveling, remote work is acceptable. It's what happens when you outside the network. Absolutely.

Bill M: 41:04 I want to get to wrap this conversation because I know you have to move on to another meeting, but I want to kind of net this out because we started with I think is fascinating seeing how your mind works from a philosophy and then how you're marrying this down to product execution and have been doing that for quite a while now with within the SonicWall world and what message have you had, if we had a message from you as far as what CIOs and CISOs really should understand from a philosophical perspective and from a technical perspective and it was just like really simple stated, how would you counsel a CIO moving forward?

Dmitriy: 41:59 Yeah. I liked how you broke down the question too philosophical and practical perspective, well in philosophical perspective i'll tell you this. Security as a problem is not going to be solved and that is not because security companies cannot do it, but because security fundamentally is the latest, network security is the latest manifestation of an age old problem of one human taking advantage of another human's mistakes. That's all that it is. And just now we live in a networked world and mistakes of one human, a software writer on their deadline have moved into this online world and that's what we will continue to live this, so there's no like final silver bullet that's going to solve the network security problem, right? As long as people continue to take advantage of other people and their mistakes, this problem will continue. That's on the philosophical level.

On the practical level, I'll say that security right now is going through the same type of ... It's a fascinating field because it changes so quickly. It's the most kind of quote unquote pedestrian analogy I can make to people, is imagine how, what sort of a revolution phones went through between 2005 and 2015. Now take that same pace and apply that to security and it's still going on. What was sufficient three years ago is just pedestrian, is just common like table stakes today. I guess I have problem being concerned using just a few words, but these are the two things on the philosophy it'll continue being a problem on practical three years ago its just table stakes now and the world's moved on, you don't use your Iphone four from 2012, It's obsolete by all standards today. Similar things go about a lot of network security products as well.
Bill M: 43:53 So to get your current thoughts on things, we're going to put a lot of your writing and your interviews and such on the blog and links out to obviously SonicWall and articles that are written about you. What are the particular products that people can go hit SonicWall about and know that you've got a hand in the execution on those products. If they're like, "Well, what's Dmitriy really doing?" What could they just hit on the website?

Dmitriy: 44:20 Sure. Look at anything that we're doing in the network security space, whether it is firewalls, RTDMI, intrusion prevention. I had my finger in it, not my hand in it, but I have to talk about client capture client and email security because email continues to also to be one of the primary ways of breaking into a network. It starts, a lot of it starts with email. [inaudible 00:44:47].

Bill M: 44:46 Yes people thought moving the 365 was going to be the panacea and they're like, "Well you didn't use Microsoft backup. Why didn't you use Microsoft email security?"

Dmitriy: 44:58 It's funny how email everybody thought that, okay, email was solved and then it's back.

Bill M: 45:03 It's back.

Dmitriy: 45:05 And its back. But it literally like you read, Sorry just one last thing. It's like, it's really, really fun to read analysis of a red teams. How red teams break into companies or the companies hire these hackers, they call them red teams and they say go test our security. And they're like, I begin by crafting an email to this organization's per blah, blah, blah. I begin by sending a bunch of emails to the employees who posted on whatever social media with their accounts. I begin by looking at what emails were compromised, what email addresses were used in the adobe breach or whatever. But it all starts with email. So anyway, I just want to make the plug for that too.

Bill M: 45:47 No, I love it. I've gone back to it recently just because holy macro, that's not gone away, but I really enjoyed our conversation, it was really cool. Also hearing about some of your mentors like Dan Geer. I'll put a link out to that as well. And getting us an idea of how you think, both philosophically and tactically is super fascinating and I know my [inaudible 00:46:10] is going to get a lot out of our conversation today. Is there any final words that you have before, I know you got to scoot out.

Dmitriy: 46:17 I just want to say thank you very much for having me. It was a pleasure talking to you and if you want me to provide fun, educational reading, I'll be more than glad to send you readings and lists and links to things that are very interesting to follow.

Bill M: 46:32 That would be fantastic and we could talk about that afterwards. That'd be great.

Dmitriy: 46:32 Sounds good, alright.

Bill M: 46:38 Thank you too, appreciate it.

Dmitriy: 46:38 Thank you for having me.

Bill M: 46:40 You got it.

Dmitriy: 46:40 Bye bye.

Bill M: 46:40 Bye.