**RedZone Podcast Episode #106: Cloud Application Security Is Your Gateway to Cloud Confidence with Shannon Emmons, Sr. Product Manager, SonicWall**

Bill: All Right Shannon, I want to welcome you to the show today.

Shannon: Thanks, Bill. So happy to be here.

Bill: We just finished a great event.

Shannon: Yes, it was awesome.

Bill: What was your experience like?

Shannon: It was really good. I love doing these kind of events and to have the audience so engaged and asking questions, like “What does the technology do?” or “What does a holistic approach look like?”, was really valuable. And you're having those one on one conversations with customers, whether they're buying your product or somebody else's. As a product manager, you get so much value from that feedback. What are they thinking? What are they looking for? What are their use cases… that maybe we've considered an edge case that isn't. So it was great.

Bill: Yes. It could be interesting from your perspective that it’s getting that pulse from the field. Yes. Let's get a sense from the questions and the answers. People have a lot of really, really good answers and good questions that you answered. It really, really worked wonderfully. How often do you do this type of field presentation and other things like that?

Shannon: I'm doing more and more of them. I joined SonicWall about a year ago and one of the reasons that I was brought on was to help launch the Cloud App Security product. As you know, until early April - late March, I didn't have a product that was available in the field. One of my conversations or one-on-one with partners, we're getting them embracing the technology. But now that we've launched and we've been out for a little bit, I'm doing a lot of partner roadshows to kind of help educate the market, not only on just the product offering but the risks to the SaaS space. I've been on the road for the last couple of weeks. You know, I’ve got more partner road shows coming up. I do as many as I can so this is the best part of my job.

Bill: Yes. Because you're really getting that feedback direct. No latency, no extraction.

Shannon: Yes. Unfiltered. Yes.

Bill: No interpretation, you can hear it live from the buyers, which is great. Let's take a couple steps back. How did you get involved in technology? Like were you always from like high school on just like down the tech path or how did this merge?

Shannon: You know it's funny, I was always on the tech path apparently unbeknownst to me, even through high school and one of my former classmates reached out to me a couple of years ago on LinkedIn and he was like, you know what, I always knew you would be in software. And I'm like, what? He was like, you re-networked everything in the entire school. Like you got all the apps running, you did and, I was like, I guess I never realized that. But it wasn't a direct career path, actually wanted to go into journalism. I did that for college for a couple of years and was very quickly bored and I wanted to get out of my parents' house. I went to work and I hired-on as an admin assistant for a VP of IT. He had always done everything himself so he wouldn't give me anything. After three weeks and ten novels later I was like, I'm sorry but I need to have something to do, or this is not going to work out for both of us.

Shannon: He handed me their help desk. I did that for a long time. I redid their help desk and kind of got into that, did some network admin. And then I joined McAfee in tech support, actually Tier-I tech support back in 2003, which feels like a million years ago now. I just kind of worked up the ranks and I spent a lot of years, eight-plus years in Tier-III as a critical escalation engineer for our large corporate customers. I worked with development and product management, and different groups throughout the company.

Shannon: Product management jobs didn't really open up in McAfee at that point very often. Then there was an opening and one of my previous PMs was like, I think you would be great and have you thought about this? I hadn't. I took the leap and it's been really good. I think coming from tech support gives you a really good balance as a product manager because you're able to really help identify pre-issues, things that you could see being a challenge for support or a challenge for customers. You can kind of avoid those upfront. It's been great. I love it.

Bill: I didn't realize the importance of product managers for vendors. I've been in the business for 27 years. We've always been on the reselling, support side of the fence and we've always interacted with SEs and sales for the vendor. But I did not really realize how important the PM, the product management vertical per product is until we began working with SonicWall. It's been really fun interacting with you on the cloud app security side and Dmitriy as well on his side. It's been kind of a door opener, that the folks here listening today. It's like this is their gateway in right up to the top, essentially and getting their feedback heard and so that's neat.

Shannon: Yes, and it gives you a really good balance. One of my former executives, mentored me quite a bit, and one of the things that he taught me, and I always come from a very customer-focused approach, but one of the things that he did teach me was focusing on the customer outcome. What's the value for the customer? Because nobody cares about your next new widget if it doesn't solve a problem. That's true. I mean it's absolutely true.

Bill: Instead of probably looking for a solution they were looking for a problem to solve.  
Shannon: Exactly. I always look at what can we bring to the customer and make their lives easier? Having worked in this space for a long time, I've seen the challenges that administrators face with multiple products and bolted on technologies and pieced together infrastructures. When I look at products and we look at business requirements as a whole within SonicWall, we look at how can we make this easiest for the customer and still solve the problem in the least amount of steps for them.

Bill: You know, that's interesting. I didn't think about that from that. You're right, sometimes the software vendors have solved it by glue ware, like we're just going to glue these two technologies together and call it our ‘new system’.

Shannon: Yes, I love cloud-ified technologies.

Bill: Cloud-ified, okay, that's another good one. Let's talk about cloud app security. In particular the problem that a CIO would have with users that want to use Box, Dropbox. Whether or not they're asking for permission or not. They're using Dropbox, OneDrive, they're using SharePoint teams. I just left the Microsoft conference and from Satya all the way down, they're talking teams. Like SharePoint was their big motherlode many years ago, teams is that for them moving forward. Literally the reps are being compensated, they want subscript, they want - what are they calling it - work load or subscriptions or something like that. They want more people on teams.

Bill: How does SonicWall fit in with helping a CIO be able to have data on their organization move into teams, move into other SaaS apps like Box? How does that work and what problems does SonicWall solve?

Shannon: Yep, that's a great question. One of the things that we see kind of across the SaaS industry and as customers make their migration to cloud, security is oftentimes an afterthought right? Particularly when you look at things like Box or Dropbox or some ad hoc ‘app of the day’, somebody needed it at that point in time and now they've used it, and your IT staff may know or they may not know. You may have company data out there that you may or may not know about at risk for a breach, data ex filtration, threat space… One of the things that we at SonicWall focus on for cloud security product is that the staff's protection space. If you're using multiple SaaS apps, if you're using something like Office 365 Suite and Box and Dropbox, or eventually Slack or eventually Salesforce, in most cases in organizations, they are managing those policies and that data in threat space differently.

Shannon: Some people assume that the cloud service providers are responsible for taking care of protecting them from threats, and they're not. They'll call it out in their contracts. It's never in big red print like we show - right, in slides, but the customer is responsible for protecting that data. If their admins are using multiple SaaS products, they increase their risk because all the products look and feel different. They all have different security controls. Most of them don't include advanced threat protection by default. They're not correlating events or getting a cohesive view across their SaaS space into what's being used, logging activity, data that's out there. They don't know if it's compliant. We really focus on a holistic approach. When we talk about protection for Office 365, we talk about the Suite. We talk about your email, your OneDrive, your SharePoint, Teams will be coming online soon.

Shannon: Ironically, I don't think I've met a person yet who really likes SharePoint. It's good that Microsoft is kind of making a push for something else. But collaboration tools are becoming more and more hot in the market and in the threat space. You can transmit files back and forth. You can share different data that are stored in the cloud most times. How do you protect that? We focus on the Suite protection in addition to other SaaS applications that you're using. You get a combined view, you get consistent policies. That reduces your risk. Everything looks and feels the same. There is no mind mapping for administrators on what does this DLP policy look like versus in SharePoint or Box or Slack.

Bill: Let's talk about policies for a second, just so everybody understands how you're defining it. Because I thought it was interesting, we had someone ask about DLP, which is just – it’s a rough... We look at order magnitudes of zero, really easy security - to 10, hard security like DLP. There's nothing about zero. It's nine or 10. It's hard.

Bill: I loved your answer to that question and part of it had to deal with policy, but maybe you can answer where you guys fit in the DLP world and what example of the policy would be.  
Shannon: Absolutely. In the context of DLP for SaaS protection, what we provide today is a very easy to use compliance based DLP. What that means is you don't need to have data classification in process. You don't need to be working on it. We provide you compliance-based templates like SOCs templates or intellectual property templates, PII, PHI, HIPAA, things along that nature. You can enable these templates with a simple check mark. We use regular expressions and we do pattern validations, account number checking, different formats. We use a series of key words. This implementation right now is not customer configurable beyond checking or unchecking the templates. You can't do the granular rules, but we also find that a lot of people get very overwhelmed-

Bill: That's what kills it.

Shannon: Yes, exactly. With a robust DLP solution and then they're overwhelmed. They don't use it and they're either sending sensitive data to the cloud and they don't know it and they're at risk, or they're in breach of compliance, or they just stopped using the SaaS app. That’s a load on them too, because we want them moving to these better infrastructures, these more updated apps, and we want to help them embrace that.

Bill: If I'm a sales rep that I'm just supposed to come up with a simple situations of a sales rep that might be a remote worker, headquarters in DC, using Salesforce, and the cloud app security. For some reason they have a document there they want to ingest into Salesforce and someone has and maybe it's a legal contract or maybe it hits one of the triggers. So, what happens to that file? Like does it just get..., if it's on its way into Salesforce from that sales reps’ laptop, does it … from Exchange, let's say are using an Exchange product from Microsoft 365… How does that whole file interaction happen? Like what goes on there.

Shannon: In the context of Salesforce, which is something we're looking at in the future. The way that it would work is similar to what we did with Office 365. We're API based technology, so we sit within the SaaS app itself. You can install our event collector to monitor activities, right, and monitor those files. Then we install a protection app as well into the SaaS space.  
When an end user uploads a file from their desktop or their phone or whatever into the SaaS app, the SaaS apps’ default security controls will engage. Whatever base AB, they provide or base for email anti-phishing or whatever, they'll engage and then everything they send up and is scanned that comes off as clean by the SaaS provider, we pick it up and we run it through all of our advanced algorithms. The advanced threat protection, if it's a file and an email attachment or anti-phishing technology, anti-spam technology to just depending on what type of data it is. But one of the advantages is that we sit within that SaaS space.  
We protect the data within the space versus it coming from a laptop or a phone or what not. As soon as it hits the APIs for the SaaS provider, we'll engage our scanning technology.

Bill: It's like a shim client of some sort. It's like a shim that sits in that... Because of their vendors opened up that API, it allows you to engage with that as that document goes in. Is it looking at the whole document or is it looking at just the email itself?

Shannon: No, it will look at the whole document. If it's just a straight file upload, we're going to pick up the file and we'll scan it with ATP. Then if you've got DLP enabled, the actions that we take on the file are dictated by the customer. If a customer has configured their policy, they want to quarantine the file, they want to send it to a vault, something of that nature that maybe they want to do nothing, they just want to alert on it, they have that flexibility to make the best business decision for them. In the context of email, what we do is when the email comes in to say Office 365, if it's got an attachment, not only are we scanning the email, we scan the emails for anti-phishing of course, and also impersonation threats. We also do advanced URL scanning, not just within the body of emails but within the attachments themselves as well. That attachment will get scanned by our capture ATP, in addition to just your regular email scanning.

Bill: We had a lot of questions about logins and login failures and then when you're in, data exfiltration out, maybe you could talk to that a little bit and talk about …. , you also called it account takeover. Okay.

Shannon: Yes. One of the concerns that we have in the SaaS app space is credential compromise. I think on a personal level, almost everybody that you talked to has had their credentials compromised in some way. I think that statistic for 2017 was 2.3 billion. Those accounts are sold in the dark web for less than a dollar, each with a guaranteed password, which is frightening. If you're an organization, you're using SaaS apps and you get compromised credentials for one of your users, that's an infiltration point into your environment. It's an infiltration point to your data - maybe it's customer data, maybe it's employee data - that data can be exfiltrated. One of the things that we provide in addition to the DLP where you can prevent sharing of external information, is also account takeover prevention. We give you visibility into your user behaviors that fall outside of their established normals.  
Shannon: We built a unique profile for every single user that uses that SaaS app. We use tons of different data points. What kind of device do they log in from? Is it a managed device, is it unmanaged, they come in through VPN and do they log in from a specific continent, how much data do they upload and how much data do they download. We build that profile and we maintain it. It evolves going forward and then anything that deviates that from that, we bring to your visibility.

Shannon: One of the things that I demo typically is geo suspicious activity. I can simulate logging in from multiple continents within a very short period of time, into my Office 365. Then the alert that the admin gets is suspected credential compromise and it will give me the IP addresses and a map of where the location is. I think you can narrow it down to within three blocks of where the IP address is. It alerts the Admin that you need to look at this. That will evolve going forward because not every anomaly is malicious. As an administrator, you want to investigate and confirm. Is that malicious behavior. But we're going to give you that quick visibility. We'll give you as much information as we can. If you're using multiple SaaS apps, we're going to correlate that activity across them. You don't have a singular app view. We know what your users’ behavior are in each of the SaaS apps they're using.

Bill: Now how is that going to be different, if someone logs in with like with Active Directory and they're just... for Microsoft, if they're logging in through AD and using MFA and conditional access, for example, where would you pick up there? I think that's my question is? How would... and that's a pure Microsoft question, but maybe it's logging into Amazon as well, but there's potentially a domain control that they're like, how do you integrate? Like is it completely separate or is it are you looking for different parameters because you're wedged into the SaaS app itself?

Shannon: We do it a couple of different ways. One, we'll try failed logins. If they're not getting through your AD, we get that event from the SaaS app itself and we'll report a failed log in attempt. Some people don't find that valuable - they want to know when somebody gets in. Where we pick up from the potential compromised account visibility perspective is when the user logs in.

Shannon: If they've already gotten through your AD or your single sign on, you've got a big problem. They've already breached that. Now we can see the log in activity, we can see the user behavior and then we bring you in that visibility. You kind of have to look at it in two different aspects, failed logins we know about them and we'll report them. We're not going to necessarily call those out as potential compromise. We give you the data to look at…  
Shannon: I had a customer last week that actually asked me to look at some of their data for them. They had an exorbitant amount of geo-suspicious login activity for failed logins. For a 60 employee company, they had 800 plus logins over a seven day period of time from all over the globe and they're in England and I think Scotland. Yes, they were like, this is not right.

Shannon: But they were concerned that somebody was attempting to get in. Like that was their approach. They hadn't got in yet, but we were bringing the visibility that somebody was attempting to get in, so it was something they could be in tune with and they could be on the lookout for.

Shannon: When somebody does get in through your other authentication mechanisms. We are there to alert you that you've got this type of suspicious activity. Maybe it's somebody pulling down large data, all of a sudden Susie started logging in at 2:00 AM, she's never done that before or she's logged on and logged off. Maybe all of a sudden multifactor authentication has suddenly become disabled, things like that.

Bill: Well, that's interesting. What about if someone, if there's an unusual, like a download of information or if someone's in an authorized way, but all of a sudden they normally average consuming 10 MEGs and now it's 25 to 30, is that a possibility?

Shannon: It is a possibility. It is something that we would want to alert you to because it would fall outside of their established norms. When the behavior deviates and it's all AI based, it's not customer configurable, today. We look to do some additional workflows in the future around that. There is the potential that it could be valid behavior, but we're going to bring it to your visibility and let you make the determination so that you can be aware because it is pretty abnormal for somebody who uploads 10 MEGs a day or downloads 10 MEGs a day to all of a sudden, pull down a 70 MEG file. Maybe it's from a different location they haven't accessed before. This is all what we would just call general weirdness. It's suspicious and you want to be on the lookout.

Bill: [5] How do you build from the AI and machine learning, we talked about this today, that we're trying to build that automated threat response so that we can confidently tackle a cloud architecture. What are your thoughts about that? Like when do you think the CIO would truly be at a point where they can feel confident treating their cloud architecture? Just like it used to be in the old fashioned data center.

Shannon: Oh Wow. That's a great question. Let me think about that one. I'm a suspicious person by nature. I’ve worked in cybersecurity probably far too long. I would never feel comfortable about anything that's outside your organization. But what I would say is this is, once you've used a tool for several months, you build a level of comfort. Anything that's AI based or machine learning based, there is going to be some nuances off the bat. It has to learn the environment, it has to learn that the behaviors to figure out what your space looks like. There's going to be some tweaks that are probably needed with any technology.

Shannon: We heard somebody today that was speaking about while they were using a different technology on their end points, they had a lot of false positives. But then when you look at their scenario, what they were doing, which change brought about, was they're actually doing hacker like activity. AI was working and machine learning was working. A lot of times we think those nuances are kind of painful, but generally when we look at them, they're actually simulating some type of bad behavior. So, do you err on the…… I'm not going to report this, or do you err on the side of caution? I think you have to get comfortable with a tool for a couple of months in your environment before you can feel really, really good and secure about your deployment.  
Shannon: I would think though that anything in the cloud, the cloud is great in somebody else's computer, you always need to be cognizant of that. Your attack surface just increased. Your attack surface is no longer inside your walls. Users are mobile, they come in from everywhere, all kinds of devices and you have to be cognizant of that. The threat landscape changes almost every day. You have to stay on top of that. Comfort is not in this industry, I don't think.

Bill: How important is Cloud App Security for SonicWall, moving forward? How much they see it as it is something that's a strategic advantage they can bring to the marketplace?

Shannon: That's a great question. One of the things that SonicWall has done in a very short period of time is expand our portfolio. The Cloud App Security space is one of those expansions. We all see, I think as many of us have worked in the tech industry for years. The move to cloud is just going to continue to increase. If we're not providing protection, somebody else is. One of the things that we look at, at SonicWall as a whole is a platform approach.

Shannon: In my previous life, I managed a product that supported a multitude of different applications. It's very hard for customers to use multiple consoles, use multiple products and you want to bring them together so that they can be more effective, they can be more efficient, they can reduce their risk. One of the approaches SonicWall has taken with the capture cloud platform is to do that. This is a piece of this because if we're not providing protection for you as a customer, whether you're using our firewalls or wireless or end point or not somebody else is and you need to be protected. Our customers that are, whether they're new customers or existing customers, we want them to have a cohesive protection strategy across their threat space.

Bill: Yes. I can't think of anything more important right now than to figure… we talked about that today, is being able to plug multiple different security lines into an overall platform. I think that it is so critical because right now there's just too many devices in the mid-market for people to watch and they don't have the capital, they don't have the talent… I mean there's a talent shortage, they don't have the resources to go tackle this all.

Bill: Settling into a platform which you can plug in different capabilities is so critical. Actually, we had talked about, while we are vested in Microsoft and people are going to be putting their... So, we have Azure at play, we have Amazon, we have AWS and I was having an interview with the CIO of Experian last week and he says, "I don't care which platform I'm on." He goes, "I'm building so I can be portable across the cloud." He goes, I want you guys... He's using Kubernetes and he's in Docker and all of these programming capabilities. I thought that is really cool.

Bill: It's a really interesting approach for a Fortune 50 or 10 whatever they may be, to be able to have the fortune to be able to just, it doesn't matter if he's in Google cloud or anything… He doesn't care. I thought, well Gosh, that has to be the vision for the mid-market is - we have to have a vision so that we don't care where people are putting their assets. Right now, we do. But Gosh, if we had this capability where you can see and govern data going into Box, Drop Box, into Microsoft, into Google, to me it would be so powerful.

Shannon: Exactly. No. Yes. You hit the nail on the head. I mean, I don't think a lot of executives staff necessarily realize the amount of console's their organization uses to manage their security posture. It's very challenging for the administrators and it's very challenging to do not only roll up reporting but get a comprehensive view across that threat space.

Shannon: One of the things that actually brought me to SonicWall is I'd worked with SonicWall peripherally as a partner for years and I've always considered them kind of a just a firewall company and they've been trying to recruit me for a while and I've kind of been probably blown them off a little.

Shannon: Then one day I was like, I should probably think about expanding. I've been here for a really long time and maybe I’m stagnating a bit. I should probably think about growing. When I went and looked at their portfolios since they had divested out of Dow, I was like, oh my gosh. I mean, I worked for a very large security player that had a very similar trajectory in terms of being acquired and being spun out and what SonicWall has been able to do and really just hone in on the capture cloud platform and just start taking it to the next level continuously, is really impressive. That's one of the reasons that I wanted to join.

Bill: Yes, it's funny the amount of momentum because we were involved with SonicWall of the early days, well for us, 2005, I think they were founded in '01. We were just involved very, very early and the team was just very assertive and they had a great growth trajectory. Then we sort of went into a bit of the dark ages with Dell and then since coming out it's just been complete momentum, which has been great because I think security needs that. It's been a lot of fun.

Bill: You won 51 awards last year, and people don't understand. It's funny, the questions coming from the audience. The space is moving quickly, but people don't sit there and just read about a vendor. Then they sit there and they actually take a step back and like, oh my gosh, you can handle the wireless, you can handle firewalls, you can handle my virtual firewalls, my web application firewalls… Now you've got cloud app security and you… Oh really? There's a difference between API security and NTA security. Did we cover that yet?

Shannon: We didn't cover that yet. No.

Bill: That's a good segue way to, oh my gosh, we got to talk about that. But then when you sit back and you go, that's a lot of capability and be able to have a limited console. I think the strategy is there and it's really fun. The API part, I actually had to dive in with my CTO because I didn't quite understand it. But now I get it. If you could explain for everybody, “What is the difference between like an NTA approach security versus like an API in the cloud world?”

Shannon: Absolutely. A couple of key differences. When you're talking about an MTA based technology, typically you're talking about an email security gateway. They sit in front of your exchange. Then they protect just email, which is fine if that's all you need. But as we've moved to the cloud and we moved to things like Office 365 that have multiple apps within that suite, you still, you have a broader need, it is not just email. Yes you need email protection. But you also need to protect your OneDrive.

I can't tell you the amount of customers that I talk to that when I asked them do they know what's in their OneDrive and how are they protecting it? They just look at me like a deer in the headlights and that's a scary place to be. You need to protect that data. You've got your SharePoint, now you've got Teams coming in and so some of the key advantages of an API based technology is not only ease of deployment, like we can actually onboard you. I think it's like six questions and when I demo it, it's like four minutes. Now, if you want to read every single line on the permission screen when we give you the popups, it's probably going to take a little bit longer. But you can get a good, you're good sampling and you're getting onboarding and then you're running your compliance scans already, within four minutes, which is huge.

Shannon: There's no latency for your end users. It's seamless to them. They don't know it's there because we sit within the SaaS app itself. There's no agents on the end points. There's no separate portal for them to log in. However they're logging into their SaaS apps today, they continue to do that.

Shannon: One of the ways that we leverage the SaaS providers, and I think I mentioned this earlier, is everything that they scan and they pass as clean, we pick it up and then we continue scanning and then we scan it with our advanced protections. The reduction in latency, because we're API based, we're really contained for the majority of the information within that same space is huge. There's no redirect of traffic that's needed. There's no changing of MX records as needed. We've used terms like CASB which is somewhat of a turnoff for people. We don't, we're not a broker so you don't have to deploy a broker, you don't have to deploy logon connectors. CASB’s also typically don't provide email protection from the security perspective.

They don't necessarily claim to be a DLP solution either.

Bill: Just your broker and carry you into wherever you're going.

Shannon: Exactly, exactly. Being API based and we don't have things to deploy, I don't like to refer to us as a CASB. We took a holistic approach to protect not only just your email but also your other SaaS apps within that suite that you're using. We focus, which is not something that your MTAs can do; and there's also deployment overhead with MTAs and there's some key differences there.

Bill: It's a nuance, but it's a very important one.

Shannon: It is. It is because that protection space has expanded. One of the things that we'd see in one of the very large enterprise customers that I've worked with is, in larger organizations their IT admins or their security admins are typically segregated. You have somebody who manages email, then you've got somebody who manages Box, somebody who manages the OneDrive and the other apps, cloud storage apps or whatever. What we didn't want to provide was a disjointed situation, right; and help the bolt-it-on approach to continue to proliferate. We did a comprehensive solution so you don't have to piece together a bunch of packages. You don't have to spend an hour and a half trying to figure out what to buy. You know your multiple IT admins can administer the same product. One administers cloud storage, one administers email. You can do all that from within the same technology.

Bill: You also made the point which I think is important is that SonicWall, like any product, has the sort of legacy reputation other than just being a firewall vendor. A good questions from the audience was, well don't I have to be on your firewall project to do this? What a great question and the answer was no, which was good.

Shannon: Yes, being API based, we don't have any dependencies from the cloud app security perspective on any of our existing products. Clearly we want you to use them and you get a lot of value from using our Capture Security Center with that single pane of glass by plugging in the different technologies and managing them from the same space. But for cloud app security, we have no other product dependencies. You just need to be using a SaaS app, like Office 365 or G Suite, or Box, or Drop Box.

Bill: Some of your other products work the same way. Like you can have any legacy investment in the firewall but might want Capture Client at your end points. Those can bypass the firewall and go right up to the security center, which I found... Though it's more powerful to kind of tie it into the firewall; but you know, if they just bought the firewalls two months ago, we’re not going to get them off of it for a little while.

Shannon: Right, right. Every customer is different and their business needs are different and nobody is going out buying an all new technology across their space in one day. It's an evolution. As a customer you get - whichever vendor you select - as many products as you can consolidate into a single platform for management and reporting and security effectiveness, the bigger benefit it is to you. Is it practical to think that every single one of our customers is going to have every piece of our technology? No. And we want to give you that flexibility so that you can manage the products that you have in a solid, cohesive way. Then if you are not happy with another technology, you can potentially replace them going forward and keep it all together in a really tightly integrated fashion.

Bill: As we wrap up here, what motivates you every day? Why do you keep at this? You saw the slide we put up there and security is… it's really fast moving. We talked about the state of the market. The audience had a choice. Are you trying to meet the vendors’ state of the market, the state of the current threat landscape or the state of the governance landscape. Where are you going? How are you managing it? It's a verb, not a noun. How do you keep your perspective and what drives you?

Shannon: Oh, you know, that's a good question. What I would say is, having survived 16 plus years in the industry, it is not for the faint of heart. It is changing every day. Threat landscape changes constantly. There is literally never a dull moment. You stay on your toes and if you're a person likes to hang out and you get comfortable in your job, this is not the industry for you. Definitely, you know? The fact that things are constantly changing, it's constantly fresh, it's constantly evolving, really helps motivate me. It keeps me from becoming stagnant and there's so many different aspects of this industry. If I want to just focus on the advanced threat protection space, or if I wanted to focus on the DLP space or if I want to go into network protection.

Shannon: There are many different facets and it gives you a lot of different ways to evolve. I think that really kind of what keeps me going and just being able to evolve, not only my career, but my thoughts and how I look at the space. My kids get real sick of me using them as Guinea pigs for presentations. They probably know a lot more about cybersecurity than they ever wish to know. Hopefully they'll pick up the torch one day. But yeah, it's a great industry. Very fast paced. I'm the kind of person who, I don't sit very long and I need that fast paced environment and it's been a good fit so far.

Bill: Everybody has a superpower. Everybody has something that they would consider their go-to strength. We're always trying to kind of fix our weaknesses. I sometimes believe that we're best, probably inclined to lean into our strengths and need to make them more powerful. Kind of looking back over your career and where you are now, where do you see your unique superpower being in your job, with your teams? With SonicWall?

Shannon: Yes. That's an interesting question. I guess I would have to say that I have an art for conveying bad information and someone can still come out smiling. Actually, when I was in Tier-III, I was known for being able to deliver the absolute worst possible customer news and still having the customer loving us at the end of the phone call. I'm not entirely sure how I've managed to achieve that. But I was, pretty much the, “Hey, if you need somebody to get back to you that needs to be told “no” or “we can't do something”, call Shannon”, she'll do it. At the end of the day you have to be truthful with people. You have to be as frank as you can. Nobody wants a bunch of smoke blown.

Shannon: I find that being truthful with people, telling them what you can do versus all the things that you can't do, right, goes a long way. They respect that and they may not like the situation, but as long as you provide the data points and the information to help them understand, they get it. They may not love you at the end. Maybe it's my Texas charm, but they still come out smiling. But yeah, I would say that's my super power. I'm not sure it's a great super power, but it is what I'm blessed with.

Bill: It's a skill for someone in product development that's had boots on the ground at a customer help desk. I mean that's the kind of person you want developing your products because they're going to see you through. They have felt the pain of having to convey information about someone's issues. So it's kind of interesting how you've gotten to the point where you are today.

Bill: Well this has been great and I really appreciate you coming down and spending time with our customers and potential customers and just talking about the threat landscape and how you're solving problems. It's been a lot of fun. Yes.

Shannon: Thanks Bill. It was so great to come out, but like I said, the best part of my job is doing these events and you guys have been such a welcoming team. You know, RedZone is always great to work with, so thank you guys.

Bill: You're welcome. Until next time.

Shannon: Absolutely.

Bill: All right.