Patrick Moorhead: Hi, this is Pat Moorhead and we're back day three of The Six Five Summit talking about one of my favorite topics, security, and even better, is we're going to talk about security and we're going to talk about AI. I'm super excited. Rob, welcome to The Six Five Summit.

Rob Greer: Thank you.

Patrick Moorhead: Thanks for doing the opener. This is the big security opener and I'm really super excited about that.

Rob Greer: Thank you. No, I appreciate it.

Patrick Moorhead: We've had some great discussions in the past and it's just amazing over the past few months how this ChatGPT phenomena has taken really the world by storm. And some people say, "Hey, I've been working on this thing for three or four years. It's not new. But boy did it capture the attention of everybody." And I know we're going to talk about generative AI and security, but I wanted to hit you upfront first by saying of really overall, does ChatGPT and technologies like this going to change maybe the future of work or the amount of people who are working on certain tasks? Let's talk a little bit big picture about this.

Rob Greer: Yes, sure. No, first off, it's an amazing innovation that is going to transform everything. It already is transforming the way that I have conversations with my kids at the dinner table. Let's just be honest and just that alone, and when people say, "Is this real?" Just ask your son or your daughter or your wife. But specifically around how is it going to change what we're used to, whether it be humans doing work or us losing jobs. This technology, AI's been around for 50 years. I think it was Dr. Weisbaum at MIT years ago looking at this and spent most of his life warning people about the implications of it. But you really look at the last 20 years when, in 2013 I think it was Two Oxford, Professor said, "Hey, we're going to lose 47% of our jobs by 2033." We're halfway into that now. We don't even have a full self-driving car. The reality is it's probably more of an enhancement to what we do as humans versus a replacement at this point.

Patrick Moorhead: We talked it's interesting. I'm just waiting for the day that I can take my word processing document, press a button, and it creates a spreadsheet or a PowerPoint document. I'll be happy at that point and maybe we can all go home then, but maybe not. But no, to your point, there have been a lot of fits and starts about when is the value really going to be there. I think eight years ago we were supposed to have a Cross Country ride an autonomous car across the United States. We still aren't there yet, but this one definitely feels real. How new is this? You talked a little bit of history, but how new is this phenomena?

Rob Greer: Well, so if you really look at it, OpenAI which is the company behind ChatGPT, it's the one that everyone is talking about. And-

Patrick Moorhead: There are others though.

Rob Greer: There are plenty of others. First off, it started off as a nonprofit. And when you're a nonprofit and you don't have to have a business case and you can go where the tech takes you and then

all of a sudden you get some smart investors and focus on some real specific business use cases and you throw workers at it and a ton of dollars as well as compute power, you see what you get with ChatGPT. And so the reality is ChatGPT I would say is very similar to what we experienced in the early days of music sharing. Remember Napster?

Patrick Moorhead: Oh, I absolutely do.

Rob Greer: Well Napster, you could argue is the forefather of streaming services today. Would you ever have guessed we'd go from that to we're talking about Disney, Disney Plus and our friends at Netflix and et cetera?

Patrick Moorhead: And Apple's made a pretty good business in streaming-

Rob Greer: Absolutely. Apple-

Patrick Moorhead: A lot of content.

Rob Greer: Figuring out a way to even take it over the top and consolidate, becoming the essential hub for all those. So I feel like we're in early innings, but we're going to see massive innovations in all fields and not just in what we're going to talk about today.

Patrick Moorhead: So Symantec in many areas of security is really at the forefront, a lot of these elements. And I'm curious, how do generative AI or ChatGPT, how does that impact security? How does it impact your world?

Rob Greer: So first off, let's just think about, it's an educational process. So most companies, when we talk with them, there's a lot of excitement. It's similar to when early days of software as a service, companies like salesforce.com found their way into organizations as unsanctioned applications. So now you have ChatGPT where people look at this as a way of accelerating their efficiency. And in a, let's say, good intentions, a lot of times those intentions mistakenly put the company at risk. And so for those who make mistakes, they tend to do things like copy data that they shouldn't or files or images into public applications such as a ChatGPT. And that is number one concern right now. Second being, when you look at copyright infringement, who owns the output of something that's your own internal IP combined with this third party public accessible service? So that one is a real big concern.

And the last one being, of course, what everyone wants to talk about on in Hollywood would be attackers. And let's be educated a little bit about where generative AI is today. It's a content development engine. At this point it's like saying you could ask a ChatGPT like system, "Tell me all the known ways to break into this type of operating system." You can't say break into these computers at these three companies. So they're not robot. It's not a robot. Now we need to be prepared that over time this technology will evolve and potentially can automatically do the things that, let's say a bad actor might want to do that otherwise would've cost them a lot more money in the past.

Patrick Moorhead: So the first two that you brought up seem almost carbon copy of what we saw with things like Box and Dropbox, the ability to share files quickly, big files while not being on the internet or not having security. The third one about this conversion, this IP creation and at that point, who owns it? If you look at the YULA, for many of these services out there, whatever you put in the cloud ends up being theirs. So I can see total issues there. And the last one I can see what we haven't talked about yet because it hasn't been productized yet, but it's coming, is having generative AI inference on the device. As you can imagine what happens, you have 100 million, 200, 500 million devices with the ability to do inference on the device as opposed to having a control point somewhere in the cloud.

And no surprise to me, things that bring greatness out there and solve huge problems, there are some bumps in the road and this is what it takes. So you meet with thousands of clients, you're offering products and services, you're at the forefront of this. What recommendations or guidelines are you giving them right now to where that it's not just... It's easy to say, and we saw this in the early days of security, which is, "Hey, what's the solution to everything?" Just make it so hard, so impossible that then everybody goes around it, right?

Rob Greer: Correct.

Patrick Moorhead: So how do we keep the train rolling of having some productive generative AI but secure the enterprise?

Rob Greer: That's very good. Well, it first starts with nothing around technology. It starts with the business policies of the organization. It's education and it's setting the foundation. And every industry's a little different. Certain highly regulated industries such as banking, you may not have a choice. They're going to come back and say, "This is not allowed. Auditors will not support that."

Patrick Moorhead: We've seen fines for using I-Messenger or a non-approved, even just a chat mechanism.

Rob Greer: Correct. And so first off, it's you go and create a policy, a business policy that you should be prepared, this is kind of the second point, to evolve it based on regulatory environment. And today actually our friends at Microsoft and OpenAI were pretty open on the fact that they're encouraging more regulation around generative AI. And so when you think about it, it's put a policy in place, educate based on what you have, but be prepared to revisit that on a regular, maybe it's every quarter. And at the board level, frankly, because this has very big implications. If you do use elements of this and something goes wrong, you still are subject to the same penalties or risks that you were prior. And then the third element frankly, is you got to put some controls in place that allow you to enforce and automate a lot of this policy, at least at a minimum monitoring.

And then if you're more sophisticated, actual automated controls. And so with Symantec, we with our DLP enterprise cloud offering, what we're able to do is help our customers say yes to generative AI tools while preventing customers from sending either images or data to these generative AI tools like ChatGPT, but still let them use it for their appropriate use cases. But this is early days. And so there's going to be a lot more technologies out there called like ChatGPT. And that's why we have a big engineering team behind us to keep us at the forefront using some of the same tools, frankly, that are powering our friends at OpenAI.

Patrick Moorhead: Rob, we both have many years of experience in the industry. We've seen a lot of waves come and go. And I'm curious, does this wave of generative AI and related to security remind you of anything we've seen in the past before, whether it be the internet, E-commerce, mobility, anything like that that we can lean on and learn from here?

Rob Greer: Well, now you're going to date me because I'm old.

Patrick Moorhead: Well, I have a few gray hairs. So we're in this together.

Rob Greer: I will say, and I could say probably we, we have gone through quite a bit. I talk to my kids about this all the time that we used to have phones that actually had a wire that's to the wall and you had to use these little... I would say the mobility cell phones and how they've become everything to what we do today. That first movement was frankly the CDMA and a lot of the pre 3G technologies and what we did with voice. I think this is even more dramatic. I probably in my lifetime, no. I got it. It's when we went from horses to cars maybe. It's probably somewhere around there.

Patrick Moorhead: It's a big deal and it's interesting. Day one when these products came out, I had a lot of people asking me, "Is this the cell phone moment?"

Rob Greer: Oh, interesting.

Patrick Moorhead: So I think you're spot on there. I had to use it first before, but after I use it... This is real. And I like to bifurcate between fads and trends, but it's definitely here. So we're early in the game as you talked about. And I'm curious if you think one side has the upper hand bad guys. I like to look at this as an AI spy versus AI spy. I'm dating myself there with spy versus spy.

Rob Greer: You might be older than me.

Patrick Moorhead: I know. But it really is kind of this one upsmanship and getting up there and now we're doing this at light speed. Who has the advantage now?

Rob Greer: Well, it's funny. If you look at the research right now, there has been no known new attacks. It's called novel new attacks created by these types of tools yet. The same type of machine learning and AI type of tools and systems that we have as the good guys so do the bad guys. And we use the same sort of tools to help identify malicious behavior as they use to create behavior. And so right now it's kind of like an arms race to some degree. So it's no different. The key is-

Patrick Moorhead: Maybe an arms race with a Deante?

Rob Greer: That's it. But really ultimately who wins? Most computing power and most data, the most data that's relevant, with the most computing power will win. And so it'll be interesting. But by no means should we be concerned that the cybersecurity companies, whether it's Symantec or others, will be taken by surprise.

Patrick Moorhead: So Rob, kind of an ancillary question here. Does any of this conversation have anything to do with this notion of zero trust? You were at RSA, you couldn't swing a cat without hitting a zero trust billboard or something like that. Is this related at all to generative AI and the threat that it can probably provide?

Rob Greer: Well, from a framework perspective, zero trust, and I tend to not subscribe to calling anything a zero-trust tool because it's a framework.

Patrick Moorhead: It's a framework.

Rob Greer: It's a framework, yes.

Patrick Moorhead: Every part of the value chain is untrusted till it is.

Rob Greer: Correct. And so in this case, and I'll just use a simple way of how I internalize it, do you trust the data that's coming out of the ChatGPT system? And so in this case, when you look at zero trust from a perspective of data and what the source of that data is, and maybe the front end system is getting from the backend is interacting with a public ChatGPT infrastructure. So when you start thinking about supply chain, the software supply chain, and in today's world, which is cloud and microservices, it's very relevant.

Patrick Moorhead: I appreciate that. Final question here. It's been a great talk by the way, and it's nice to know we share some of the same timeframe and can relate.

Rob Greer: Thank you.

Patrick Moorhead: I'm not looking for specific product announcements here, but more what is your approach to generative AI in the product line as you map this out in the future? What is just the strategy or the approach? Not looking for specifics, you just spill before announcements come.

Rob Greer: Well, first off, it's not a question of if you use generative AI, it's a win, and frankly our customers, if you're not leveraging this technology, you are considered a legacy. Let's just be frank. And why? Because it has real world use cases that are tangible now, kind of like when you think about the iPod, and the reason it was successful with the iTunes store is it took something no one could understand, which was PKI, and it actually instantiated in something everyone can associate with, which is I no longer need these DVDs anymore or even have to manage my own, let's say, pirated music. When you think about our products and what our customers expect, first off the simple things, do I need to go read an administrative manual to go figure out how to do something or should I just ask my personal assistant, personal semantic enterprise cloud assistant?

So the low hanging fruit, frankly, is traditional tech support, administrative support, how to best practices and auto policy creation. We put our customers through quite challenging policy creation exercises and so do our competitors. So I think from an ease of use, less mistakes, now let's not kid ourselves, if you just let the AI go by itself, it's like letting your 16-year old with the Ferrari-

Patrick Moorhead: Exactly.

Rob Greer: By his or herself. So you need oversight because, frankly, a lot of times that system is wrong. So first off, that's the low hanging fruit. As well as because we're a security company, we need to be using this technology to better keep up with the vulnerabilities and exploits that are out there. And so that's just a no-brainer. We're already been using AI for years. The generative aspect of this and the ability to use it in use cases that a typical administrator or even end user can, that's where we need to take it.

Patrick Moorhead: And for what it's worth, your cloud-based approach seems to me would give you an advantage to be able to implement all of the newer features sooner. So I don't want to put words in your mouth, but…

Rob Greer: Absolutely.

Patrick Moorhead: That strategic move that you made, that's where it's all happening.

Rob Greer: We've invested a lot working with one of the top hyperscalers in the world to help us accelerate that transition. And we are at, I would say, a competitive advantage to others who are providing similar services. Not only because we do it in the cloud, but we also are able to do it simultaneously for the on-premise workloads, which by the way, these big companies, they can't just turn off their old networks and just go straight to the cloud.

Patrick Moorhead: Exactly.

Rob Greer: And you need to do it with one common policy, one common set of context across all those different complicated use cases.

Patrick Moorhead: That's great. Rob, I really want to thank you for opening up the security track here at The Six Five Summit 2023.

Rob Greer: Appreciate it.

Patrick Moorhead: Combining two of our favorite topics which are security and AI and maybe a little bit of multi-cloud in there too.

Rob Greer: Oh, absolutely. Everything's a multi-cloud use case. There's just a lot of companies don't articulate what that means. And the reality is when you're talking about large organizations, they don't have the luxury of just dealing with one workload, one cloud.

Patrick Moorhead: We're definitely on the same page. I'm glad we're here. I like to look at the cloud as a teenager. It's 19 years old. And if you're 19, you're mature, but you're not making all the right moves. You're not making all the right decisions.

Rob Greer: I did. I made all the right moves.

Patrick Moorhead: I didn't. But I'm glad we're at a time where at least we're acknowledging that it's not just if the multi-cloud is there, it's here and enterprises are doing it. I have yet to talk to a Fortune 500 enterprise that doesn't have multiple IS providers. And that by definition is multi-cloud.

Rob Greer: Absolutely. That's great.

Patrick Moorhead: So you got to get the verbiage there and the belief and now we're working at all the solutions that support the multi-cloud. So anyways, thanks for coming in the show. Really appreciate it.

Rob Greer: Thank you very much, Pat.

Patrick Moorhead: So this is Pat Moorhead signing off for this opener for the security tracks Six Five Summit 2023. Well hope you tune in and listen to the other awesome security content we have. And don't forget, we have a day one and a day two. You can go back and watch at your leisure. Take care. Thanks again.