ML/AI's Role in Securing the New Endpoint Attack Surface with Dell Technologies

Shelly Kramer: Hello and welcome to this session of the Six Five Summit. I'm your host Shelly Kramer and I'm joined today by David Konetski from Dell Technologies. Our conversation today is going to be focused on ML and AI and their role in securing new endpoint attack surfaces. So as a prelude, when you think about Dell Technologies and security, you might think about desktop or laptop, what kind of hardware someone might be using. But we're here today to talk about the security journey as a whole, and sort of the security posture that protects endpoint devices throughout all aspects of the hardware journey.

So with that, David, it's great to have you today. Welcome.

Dave Konetski: Great to be here.

Shelly Kramer: Absolutely. So tell me a little bit about your role at Dell Technologies.

Dave Konetski: Absolutely. Hello, everyone. My name is David Konetski. I'm a Fellow in the Client Solutions Group at Dell Technologies. We drive technology strategy, we drive technology innovations, and we're the ones that provide differentiation into the product set. And so today, like Shelly said, we'd love to talk about security and AI, and how that applies to security. And it's funny, you mentioned that Dell Technologies is not necessarily considered a security company. And I like to think that we are not only a security company.

Shelly Kramer: Absolutely.

Dave Konetski: Dell Technologies is all about providing solutions to our customers to empower them to reach their missions, and also advance human progress.

Shelly Kramer: Absolutely.

Dave Konetski: Providing those solutions, security is an inherent piece of that solution. Matter of fact, we call it intrinsic security because as you all know, the word intrinsic means essential and naturally belonging to.

Shelly Kramer: Well, and I like to think of security, and I think that everyone should think about security as foundational. Every product, every process, everything needs to be built on a foundation with a security first mindset. And I think that's similar to the concept of intrinsic as well.

Dave Konetski: Absolutely. And we really take that approach. We have a fairly unique position in the industry in that we produce the hardware. So therefore, we develop and we control the firmware and the underlying operating environment that sits below the OS, and we can start there and create a secure foundation.

And when I talk about as being security company, I look back historically, and we have a long history of pioneering in security. We were the first PC OEM to put TPMs, or the trusted platform module, on motherboards. We were the first in, we are still the only company that shipped a dedicated security processor to secure identities. And as we look forward to what we're doing now, and we're advancing all those capabilities, we're taking our BIOS and firmware protections, and now producing indicators of attack below the OS. We're doing off host verification to make sure that the platform is in a perfect shape and tested before we boot. So as you can see, we're very focused on providing that secure foundation. But then, of course, that's...

I'm sorry. Go ahead, Shelly.

Shelly Kramer: And really, you mentioned above and below the operating system.

Dave Konetski: Yeah.

Shelly Kramer: So I want to focus on that for just a minute. Can you explain more for us, what that means and how that impacts a customer's security posture overall?

Dave Konetski: Yeah, absolutely. So as I mentioned, we provide that secure foundation, but that's of course not all. Now the environment, the operating environment, then includes the operating system and the applications. And of course, everybody's moving to cloud native applications, as well.

Shelly Kramer: Right.

Dave Konetski: So what do you do to build on that strong foundation to protect yourself? Well, you have to have industry leading state-of-the-art advanced threat protection platforms. You need to have security monitoring services that watch your network and your end points and your cloud access to be able to generate insights. And you have to have that cloud access protection in place. And we do that through partners.

So our security monitoring is of course, with one of our Dell Technologies companies, SecureWorks, industry-leading managed services and, now, software platform provider. And then we partnered with folks like Netskope for a cloud access security brokering, and Carbon Black for advanced threat protection systems. And all of those, as we'll talk about in a minute, use artificial

intelligence, that is machine learning and deep learning, to be able to keep one step ahead of the adversaries.

Shelly Kramer: And that's what I want to talk about now. So talk with us a little bit about AI and ML, and the role they're playing in the security landscape and how we're using them.

Dave Konetski: Yeah, absolutely. Thank you. So of course, AI is the umbrella term of four things that we do to analyze complex data sets. And tools like machine learning and deep learning have evolved to the point where it is enabling us to use them in interesting ways to give us the target to go look for. I want to make sure everybody understands that AI is not the only bullet in a gun, so to speak. It's a tool. It's a tool that makes it possible to stay ahead of the adversaries, and I'll describe that in just a moment. But as you analyze complex data sets, you're able to then generate patterns of good behavior so that you can then look for anomalies. You can analyze that behavior and then look for indicators of potentially malicious attack.

Shelly Kramer: Right.

Dave Konetski: And then, we can take all of the events that we have, and to quote SecureWorks, they have billions and billions of events, upwards of 7 billion events that come in daily. And you have to filter that down into meaningful events or meaningful insights that you can then put into the chain. You need to have your researchers that develop algorithms and take advantage of artificial intelligence. Then you need to have your security analysts who take those insights and figure out what are your targets to go remediate. And then of course, you have to have your developers that are building the platform for all of this to run.

So when I look at AI, like I said, it's a fantastic tool for us. But our adversaries are also using AI to be able to try to infiltrate our infrastructure, which is a very interesting opposite effect of the usage of AI.

Shelly Kramer: Yeah, absolutely. And I'm going to hold off on talking about that. I think we're going to wrap up our conversation with, sort of, look at that and what's ahead.

So one of the things that you mentioned, having access to real time insights, and we've partnered with Dell in the last year and done some research focused on security and the hardware journey and that sort of thing. And one of the things... I don't have the exact data points in my mind. But one of the things that we looked at is, when we talked to IT leaders charged with security operations, they absolutely knew how many attacks they had and they knew what to expect, and everything else. And the people who had their finger on the pulse of

what was actually happening on a daily basis, and what they expected to happen moving forward, where people who were using dashboards that afforded them real-time insights into security operations of what was going on.

And conversely, when we spoke with folks in IT who weren't using that kind of technology, or any technology to be able to allow them access into the system, they had a very sort of Pollyanna-ish attitude in that, "Oh, we think we're good, and we haven't had any threats or anything like that." So it really is very interesting. But we are big believers here at Futurum that you don't know what you can't see. And to operate without the benefit of actual insight into what's happening on a minute by minute, hour by hour basis, as it relates to your systems is not really very smart.

Dave Konetski: That's right.

Shelly Kramer: And more importantly, really dangerous.

Dave Konetski: That's right. And so I talked about our ability to generate indicators of attack below the OS. I talked about our partners like SecureWorks and Netskope using artificial intelligence to look for anomalies, look for detectors of malicious activity. Those are all just indicators, though. And your point, those indicators have to be surfaced up into a security analytics platform so that the security practitioners can analyze those events that are determined to be the most valuable events, and then take action. Whether it's just determining that it's not malicious behavior. But if it is, then unpacking it, doing forensics, figuring out where the adversary came in, how they got in, how long they were there. And then, as I usually put it, is then cleaning up the mess, right? Removing them from the environment. Putting solutions or putting protections in place so that it doesn't happen again, should there have been a bowl vulnerability that was detected. And then of course, putting your monitoring systems in place so that you can make sure that you don't have that kind of breach again.

But to your point, that security analytics platform has to be robust and it has to be clear and it has to point you to the events and the indicators are the most important for you to be addressing.

Shelly Kramer: Yeah, absolutely.

Dave Konetski: A great example is security indicator that zero history of anyone using it in the past is probably a little less important, or urgent, I should say, than one that is known to be a vulnerability that is being exploited at the current time. Having that insight is very important to understand how you attack the problem.

Shelly Kramer: Yeah. And the thing, too, about the benefits of machine learning and AI that I don't think we touched on is the ability for continuous learning. As the systems look at the data, sees this massive amount of data coming in, the system automatically gets smarter. And so you want to talk about that a little bit? I don't want to... There's so much about this that I don't know the specifics of, but I know that's a huge benefit of AI and ML.

Dave Konetski: Oh, absolutely. And then, so I talked about at the very highest level, that using AI to do analysis of complex datasets, to be able to generate known patterns of good behavior, patterns of malicious behavior, be able to form detectors... As SecureWorks works, they have a set of detectors that pull out insights. But the thing is the trap that many fall into is to think that once you have an algorithm in place and you're analyzing a dataset, that you're now in steady state. The reality is that that data set continues to evolve.

Shelly Kramer: Right.

Dave Konetski: The reality is that adversaries are continuing to watch the environment to figure out how they can either stay, metaphorically, below the radar, or how they can mimic the behavior of authorized users. So your algorithms or your analysis has to continue to evolve. And so that's the whole circle of generating insights, using those insights, doing forensics, and then feeding that information back into the model. So the model is never done.

And we also have to get comfortable with the fact that the model is never done. Like any good engineer, like any good data scientist, they always want to try and find that perfect algorithm or that perfect, you know, get the perfect data set so that they can come up with the right answer. And I'm a firm believer that in many forms of engineering and especially security, we are going to have a great answer.

Shelly Kramer: Today.

Dave Konetski: But it miht not be the perfect answer.

Shelly Kramer: Well, I don't know that it's perfect. Maybe it's perfect. What I'm thinking about is finished. Right? And I think that... We talk about this a lot as it relates to digital transformation. And sometimes people are surprised when I say your digital transformation journey is never done. It is a journey and technology has evolved at an incredibly rapid pace. By the way, it will continue to do so. And so, what our mission today, whether you're an engineer, whether you're an analyst, or whether you're a project manager, our mission in the world today is to understand that change is a constant and evolution is a constant, and these journeys are ongoing, and we use technology to help us do better and be

smarter and do things more rapidly than we can do ourselves and all of that sort of thing. But we're always going to be evolving and changing and testing and measuring and implementing. And for those of us who love change, that's exciting. For those of us who don't love change and who want that perfect ending, it requires a little bit of a change in mindset.

Dave Konetski: That's right. And what you just said reminds me of something, also, is that perfect ending... I mean, we look at artificial intelligence in different ways. And some of it, also, is the application of ML and deep learning to create responses. So it's one thing to know when you have... None of those is a problem, but sometimes when you have, let's say, it is a breach. Other times, you just have an inefficiency in your process. Being able to apply AI to an automation system so that you can analyze the insights that are being generated, and then generate the right response, starts to free up IT personnel to be able to attack the more difficult problems, digital transformation problems, in their environment.

And right now we're in an interesting state in that everybody's interested in automation, but they don't want to let go. So it's like, "Yes, give me the automation, but let me hit the button." And eventually, if we have this conversation three years from now, I'm sure we'll be having a very different conversation, because professionals are becoming much more comfortable with automation and letting the system, and trusting the system, the system that they have given policy to, and that the automation is actually going to benefit their users. And you have to do that automation in a way that it doesn't stop or limit productivity. It actually encourages productivity. And it may have users working differently than they're used to working. You may go from a local session to a remote session. You may go from one cloud access to a different device, cloud access on a different device. But the point is that through automation and remediation, we're going to be able to fix all of your problems in a transparent way and keep you productive.

Shelly Kramer: Well, and yeah, and when you can use automation to kind of get rid of... You don't rid of them. They're being handled in a different way. Those mundane, those repetitive tasks that take time and attention, and we're just so used to doing those things that when you factor that out, it's so exciting to see people... I mean, we do a lot of work in the automation space, and it's so exciting to see people talk about the trepidation that they had going into their automation journey. And then, talking with them a few months later and it's just like, "Oh, my gosh." And their eyes are opened as to the possibilities here. And, "Now we've been able to do this, but what about if we automate this?" And it really is kind of getting that toe in the water and taking a little bit of a dive and a little bit of a leap of faith. "Oh, this technology really is pretty cool."

But it's exciting to see people progress along that journey. And also really exciting to see them being able to focus on, as you said, the more mission critical tasks, the things that require humans and critical thinking and that sort of thing. So it really is... We're at an interesting part of our journey right now, especially as it relates to automation and the benefits of AI and ML, that it can bring, for sure.

Dave Konetski: Absolutely right. And when I think about what we are working on for the future of compute, and the way things are going to evolve and change, we're going to have many of the mundane tasks automated, and we're going to have the delivery of workspaces being a very different paradigm. That changes the whole security game.

Shelly Kramer: Right.

Dave Konetski: Where we used to be focused on securing the platform and securing a desktop and security applications running on that desktop, that whole paradigm is changing. And we see it with cloud native applications today, and that will continue to evolve. And as we become more automated and flexible, you'll see the workspaces evolve with the user, and based on their context or their security posture of the device they're on, what their entitlements are, and what they're allowed to do, there'll be delivered a dynamic workspace that will move with them, and it'll follow them through their day. And that changes the whole security paradigm.

No longer can I count on a classic desktop-based advanced threat protection systems. I now have to be much more concerned about protecting cloud access, protecting usage patterns in the cloud, which is where, I talked about, we've started to pioneer the automation or the AI placed onto cloud access, file access, and user behavior in that realm because your telemetry changes, right? It comes from your workspace. It no longer comes from a set platform.

And so, again, to your point, people are going to have to evolve. They're going to have to be comfortable with change. They're going to have to be comfortable with coming up with a great answer and then iterating on that answer as we learn more.

Shelly Kramer: Right. Well, I have confidence we'll get there. It'll just be different.

Dave Konetski: Great. That's right.

Shelly Kramer: And you know what? We really have no choice. It's not a matter of you either are on team change or team no change. It's really that we all need to be on team change, because there really is not another option.

So I would love to talk a little bit about supply chain. And we talked earlier about intrinsic security and how Dell Technology builds security into its hardware above and below the OS. But what about supply chain?

Dave Konetski: I'm glad you brought that up. So take that metaphor again. That we're building a house or we're building an environment based on a secure foundation and then layering our productivity tools on top. But how did that environment get developed? How did that environment get delivered? we really need to go back. That's why supply chain security is so important. The security of the device in the workspace itself is a result of everything that happened before.

So at Dell, we go all the way back to, of course, you have to have a world-class secure development life cycle. So as you're developing the tools and as you're developing the software and the hardware, you're building in that security, again, intrinsically into the platform and into the software. Then when it's developed, how is it delivered? Making sure that we have tamper-proof containers and tamper-proof boxes. And now we've even advanced that further so that we can start to do programmatic verification of pieces in the device itself. So we can make sure that what landed at the customer site is what was built in the factory. We've launched that with our PowerEdge servers and we're going to continue to advance that capability.

And then as we go forward, being able to do a verification at a station, and then of course, remediation, so that cyber resilience becomes a part of the supply chain. And so, as you can see, it's not one person's job, right? Everyone has to think about secure supply chain. Everybody has to think about security intrinsically built into the products. And our customers expect us to deliver secure and testable products to them. And that's something they shouldn't have to worry about. And that's something where we excel, and differentiates Dell.

Shelly Kramer: We've done some research with SAS in the last couple of years, a couple of different research studies. And we talked with 4,000 people, 2000 from the brand side and 2000 from the consumer side. And one of the things that came through loud and clear from consumers is security, privacy and security. And they feel very much like it's a runaway train and something about which they have absolutely no control, but quite a lot of fear about, which is understandable and justified. But I think that from the brand side, when you approach this with a... Again, security is a foundational thing, and when customers understand that everything a company does is with a security first mindset, I think that goes a long way toward allaying their fears that this... You know, it really is a very big problem on the consumer side. So I think that it's an important part of what it is Dell Technologies or any company does, is to really lean into all things security, because it is something that is top of mind for most consumers.

Dave Konetski: Oh, absolutely. And as we watch what's going on in small business today, the way we approach small businesses the same way that we approach consumer. Of course, as I'm sure a lot of you heard, small business is a fairly large target for cyber adversaries. They have less sophistication and usually have less protections in place.

Shelly Kramer: Right.

Dave Konetski: So Dell is really focused on small business and providing them solutions, and mostly turnkey solutions. So that we don't rely on the fact that they have security practitioners because often they don't. That looks just like a consumer. And so it would be very easy for us. Our global services today are organized so that we can have [inaudible] small business, very small number of people in a tenant. And that's the infrastructure that you need. That doesn't exist a lot of places, to be able to approach the consumer security problem.

Shelly Kramer: Right.

Dave Konetski: Our vision is that consumer and small business environment should be a complete no worry, no touch, kind of zero IT kind of thing. We take care of that for you, because that's where we bring value.

Shelly Kramer: Speaking of small businesses, actually businesses of all size, and we started talking about this a little bit earlier, but you can't read any of your news sources today without hearing of yet another ransomware attack, or another hacking. And we're coming off of the massive Colonial Pipeline attack, and we're still finding damage as it relates to the Solar Winds attack and the Microsoft Exchange. I mean, it's just like the list is so long. But I want to talk a little bit about the cybersecurity space, and the reality that this is big business for threat actors, and there's so much money to be made. And so I'd love to talk just a minute as we wrap up our conversation about what's happening, what our adversaries are doing as it relates specifically to the use of sophisticated technology like AI and ML, and how do we counter that?

Dave Konetski: Yeah. It's certainly evolved over the last many years. And we used to approach it, security analysts used to approach it, and try to cluster adversarial behavior, or cyber criminal approaches. And that is becoming more and more ineffectual. The reason is that cyber adversaries are becoming much more sophisticated, and they're changing their approach. They're changing their modus operandi on every single attack. So it's difficult to pattern that malicious behavior end to end, and then reapply it to a new attack. What you have to do is break that up into... As I mentioned before, SecureWorks, uses detectors. So break that up into the components of an attack and be able to put those components together to define malicious behavior.

The adversaries are using AI, certainly deep learning, to analyze a tremendous amount of data coming from end points because end points do represent a large majority of the initial attack points in [crosstalk].

Shelly Kramer: Right.

Dave Konetski: And so they're using AI to be able to do analysis to figure out what does this person's behavior look like? And how can I model that person's behavior while I'm getting into the systems that I need to get into? Obviously, the thing that's a consistent piece of the attack through many of these recent breaches is, whether it be stolen credentials or living off the land, acting as an authorized user.

Shelly Kramer: Right.

Dave Konetski: And so, the way that we need to combat that, to stay ahead of them, is to be able to watch for that anomalous activity. Because even though they're acting like that authorized user, they're not doing everything in a way that that authorized user would do it, because obviously they're trying to get to systems that that person or persons may not naturally have access to, or data that they don't naturally exfiltrate from their resting places. And so watching things like that, as well as many other indicators, will give us a step ahead, find out when they're in the environment. Because usually, especially with these larger ones, there's a dwell time between the time that the adversary establishes themselves in the enterprise until they actually launch the attack. And the goal is to identify them in the network and remove them from the network before they're able to launch the attack.

Shelly Kramer: Important stuff.

Dave Konetski: Yeah.

Shelly Kramer: Well David Konetski, thank you so much for joining me this morning and talking about what's going on with Dell Technologies and security, and specifically the focus that you are shining on AI and ML in security systems. I think it's always a fascinating conversation, and I really appreciate you joining us in this Six Five Summit event. Thank you very much.

Dave Konetski: Thank you, Shelley. It's great being here.

Shelly Kramer: This is Shelly Kramer from Futurum Research. Thank you for joining this session of the Six Five Summit, focused on AI, machine learning, and business development. The conversation with Dell Technologies' David Konetski was a

fascinating one, and we've got one more session today, featuring Tom Anderson, the VP of Red Hat's Ansible Automation Platform.

We then finish off the day with a live Q&A featuring Splunk's president and CEO, Doug Merritt, Kumar Sreekanti, the CEO and head of software for HPE, Mick Hollison, the president of Cloudera, and of course, Futurum's Daniel Newman, and Patrick Moorhead of Moor Insights and Strategy. This is one conversation you'll want to be sure and be a part of so check your agenda for a link to view and participate. We'll see you there.