Commvault RSA 2026 Chris Bevil

Fri, Apr 10, 2026 10:37AM 12:39

SUMMARY KEYWORDS

RSA 2026, Commvault, Chris Bevil, cyber security, AI enabled recovery, res ops, ransomware, AI detection, cyber resilience, recovery as code, Active Directory, Okta partnership, cloud identity, data recovery, incident response.

SPEAKERS

Jo Peterson, Chris Bevil, David Linthicum

J **Jo Peterson** 00:00

Hey everyone, thank you so much for joining this edition of clear tech loop. It is a special edition with our friends at Commvault getting ready for RSA. We've got Chris bevel, Practice Lead for cyber security and AI visiting with us today. Hey, Chris,

C **Chris Bevil** 00:15

Hey Jo, it's nice to meet you. And David,

J **Jo Peterson** 00:18

nice to meet you as well, and glad that you could join us and Dave lithicum, my friend, well known cloud and security expert, and we're just going to take a couple minutes and chat through some questions here with Chris. So let me go first. How does res ops bring together security and operational teams for improved AI enabled recovery.

C Chris Bevil 00:45

Yeah, Jo, that's a great question. And you know, when I think about res ops, I really think about it as solving a problem a lot of organizations have really had for a long time. If you think about it, when you look at an organization, security teams and operation teams are both critical, but usually they're coming at something in different directions. And when you when I start, then starting to think about, okay, that's how we normally work. If a ransomware attacks, and we continue in our normal methodology, and we have this major disruption that occurs, what will generally happen is we're all running in two different different directions. You know, security might say, We found an issue. And, you know, backups are in this IT security people may say, Well, you know, we have backups. And the problem is everybody's running in different directions. What res ops does is it really gets everybody focused in one line. It gets security and operations and the identity and all the teams, really as a whole, to just start thinking in one focus. And that way we can have real recoverability, if you will, because we all are marching to the same beat. We've practiced, we've tested with chaos. We know what we're supposed to do, and through that, we're all working as one. You know, one team

J Jo Peterson 02:07

sounds like a better approach.

C Chris Bevil 02:09

It's a much better approach. I know you've lived the CISO world as well as I have. And you know, if you've ever unfortunately lived through an incident, you know what happens? Everybody's going in 100 different ways. We eat lots of pizza and we have, you know, a stinky room that we're all hanging out in. And the reality is, if we all work together and we all knew what we needed to do, from our instant response plan to our cyber recovery plan to our cyber resilience plan, and on and on, then what happens is, we all work together, and it's just a much better outcome across the board for everyone.

J Jo Peterson 02:44

So are you saying we get less pizza? That's what I'm trying to understand.

C Chris Bevil 02:48

Well, I could probably do without more pizza, but yeah, I would, let's hope that we could get less pizza. I think that would actually work for us.

D David Linthicum 02:56

Alright, alright. I got a tougher one. So the combo res op solution provides AI enabled proactive detection and defense as organizations invest more and more in AI, what's included in that detection and defense and how can this security really move the needle for clients?

C Chris Bevil 03:17

How come Jo got the easy question. I think the, I think the best way to answer that is really, David is starting by keeping it real. Because really, this is not about throwing AI on a slide and pretending that someone saw some kind of cyber resilience thing, and it's it's also not about going in and replacing somebody's security stack. If you think about it, the real value is whether AI helps customers make better decisions faster and when things are going sideways. And with our res ops model, AI enabled protection and detection and defense is really about bringing all of that together. It's bringing our signals. It's doing a lot of other components for us, so that we can really see a lot easier. How you know the identity behavior is there. We can see what privilege escalation, configuration, drift. It just brings everything together. If you think about it. When we look and think about AI now and you look at an x ray, we're seeing things that AI is seeing things doctors can't, and that's what's happening in the cyber security way, is what you know world as well. It's just things that we would overlook as time goes on. And obviously with AI, I could, I could talk for days on this, because really, you know, any of those by themselves looks just like any other alert, like I was saying a minute ago. But when you can connect them all together and tie them together, you begin to see that little crack on that bone. You begin to see the things that really you didn't know were there before. And it really allows you to start seeing a seeing a very clear, clean, trusted and safe path. Forward. So that's, that's how AI is really beginning to help us think through things. And, you know, like, I kind of like to, you know, use another analogy, where, when I'm thinking about AI, if you go back to the Winter Olympics and you think about that downhill skier, they have a spotter or coach that's always really trying to talk them through and tell them on the run where they're trying to go, what they're trying to understand, to spot those dangers. And really, I think that AI and AI and resilience is that as well. It doesn't replace the people, but it really helps them see more of what we're trying to do just more clearly, and it helps us make decisions better and faster.

D David Linthicum 05:45

Yeah, it's taking advantage of the dynamic capabilities of AI. I think that's, that's kind of core to this, and that's something that's going to have to be happening because you're, you're, in essence, spy versus spy, fighting fire with fire, and you have to have a be able to match it up with with something that's going to be, you know, provide the resilience. So next question, working with the comm ball team, I know that you folks are about continuous validation improvement. So what is the concept of recovery as code or Roc?

C Chris Bevil 06:16

Yeah, I really like this. When you listen to it, though it sounds super duper technical, doesn't it? And if I'm supposed to be talking super duper technical, we're in a world of hurt. You know, I'm that CISO that came from the GRC side. So we like to try to make things a little bit more straightforward. And actually it is, if you think about recovery and code, it basically really means recovery should not live in some weird, dusty, old run book, or have some tribal knowledge, you know, with that, that guy that's got the knowledge in his head, we all have that one, and he winds up being on the cruise when we're when we're having an event or something, you know. But it's that one, you know, one thing that we want to think about, and it's, it's really just not a great model in the way I just described. Now flip that, and if you think about it, and the idea of recovery should be structured, it should be repeatable. We should be able to test when we start thinking about that, then we kind of think about infrastructure as a code. So we're kind of beginning to make it easier. So now we say, I think, I know, you know, I can rebuild this, and you're actually codifying those dependencies that we have. We get to look at our operations different, our workflows function more. And it just really allows us to recover a lot back, a lot better. And it's, it's really a more modern recovery strategy that really lets us think about how we get our data back, but most importantly, how we get our data back cleanly, and we get it back in the most efficient and efficient, effective way. You know, a lot of people say, oh, when a cyber event occurs, or something occurs, RPO and RTO go out the window. They kind of do. But the reality is what really we're saying is they're still there. We want to get back to that recovery point, that recovery time quick, but we got to have all that data coming in clean and we've got to make sure that all of that works together, so that when we pull the trigger, and we come out of those clean rooms, and we come out into these different components, and our apps come back, and our identity comes back. It's clean so that we can turn it on. Does that make sense? I tell you, I get kind of excited about it. I'm trying to not use all my analogies that I could can't use them yet on you anyway.

D David Linthicum 08:31

Makes fine sense to me.

J Jo Peterson 08:34

Yeah. So, so Chris, last year at RSA, I got to sit into in the live ransomware event where we recovered, and it got me thinking a lot. And, you know, I thought, gosh, you know, if applications go down, what's the first one to come back up? And how do we know if it's good or not, right? So for folks that are not familiar with Active Directory resilience. What is that?

C Chris Bevil 09:05

Well, let's, let's think about Active Directory as a whole. It's kind of the brain of the group, because that's, that's where everything lives when you're an organization, if I'm a bad guy, and I can get to Active Directory, I can go anywhere, I I can go anywhere I want to go. And that gives me the keys to the kingdom. So, you know, I simply think about Active Directory, really resilience as it is, is really about restoring that identity, that because that active directory has everybody's identity, it's, it's, you know, it's the keys to the kingdom. And when we begin to look at control plane access and privilege and policy and trust across the environment. It, you know, we want to be able to bring that back, and that's the thing that we got to bring back first, if possible. And so that's where we really try to encourage a lot of people to think about when I. I need to come back, what's, what's the most important crown jewel that you can have, and that is Active Directory. Because once I get Active Directory restored, it's good. But here's the kicker, getting active directory restored, it still has to be clean. You've still got to make sure that nobody's there. I heard a story last week at the hems national conference, and somebody was telling their story, oh, we got all clean. We got everything back up. We knew we were ready to go, but we forgot to look in our Active Directory, and the bad guy was right back again. So just restoring that server is not enough, and just, you know, bring an Active Directory is not not enough, but bringing true, clean, Active Directory methodology into how you come back is critical, and that means being able to identify those bad changes that were in Active Directory, making sure that the right objects and settings are done, because what the bad guys want to do is they just want to change it all. And you know, to kind of give you the final story on the story, they told us, Jo, it was really interesting, the guy that was one of the guys that kept his admin password off system, and they were lucky, because they had been blocked out and he had violated the policy of the organization. But luckily, the password had not been changed, so he was able to get in, and they were beginning to pull things back. So he got an award for, you know, breaking the policy in the beginning. But the reality is Active Directory is critical, and you know, now we're actually going to be extending into Okta as well.

J Jo Peterson 11:36

So I saw, I thought, that's great, because so many enterprises have Okta. So tell us what that's going to let a customer that has Okta do in the event of a ransomware attack?

C Chris Bevil 11:49

Yeah, it's going to, it's going to get us even more relevant, because identity today doesn't just always sit on prem anymore, and a lot of organizations are operating around active directory and cloud identity systems. So when we begin to partner with Okta, you know, we're going to be able to help really overcome a lot of those challenges that our folks will normally see. And we're really looking forward to the partnership with Okta.

J Jo Peterson 12:16

That's awesome. Well, lots of exciting things happening at RSA, y'all come see our friends at combo. At RSA, Chris will be there. Michael Filo, lots of the lots of the great combo team is going to be there, and we hope to see you too. So thank you for joining today. You.