HOW BLACKBERRY USES BMC DISCOVERY TO KNOW EVERYTHING IN ITS GLOBAL ENVIRONMENT

In this Run and Reinvent podcast, I chat with Greg Sacrey, principal application architect at BlackBerry, about the importance of knowing what you have in your environment, whether it's on-premise or in the cloud. Below is a condensed transcript of the conversation.

Andy McCall: For those that might be unfamiliar, can you tell us a little bit about BlackBerry and what you're doing?

Greg Sacrey: BlackBerry itself, people may or may not be aware, that we were always a huge in the smartphone industry, we're not a smartphone company anymore, we're absolutely a security software. Our aim is to secure the smartphone experiences as well as the Internet of Things. That's where our main focus has been.

Andy: Could you maybe tell us a little bit more about the current IT environment you are dealing with and particular your relationship to BMC Discovery and how it's used?

Greg: Our IT environment is very large. It has shrunk over the years as we adopted more virtualization. We run a large private cloud. We are involved in public cloud, as well. We have we have presence in Azure and AWS currently, as well as our private cloud. So, with that, we have things kind of stretched all over the place and our environment is also geographically dispersed. That's where the BMC Helix Discovery really came in a play. When you have this many things, you need to be able to keep track of what you have or what you don't have. And that's where Discovery

came in because we have tens of thousands of endpoints and you can't just track that easily. So, the automation that BMC Discovery allows that we can go into and truly discover what we have.

Andy: Given BlackBerry's security focus are the key things that Discovery has helped you with in that particular field?

Greg: If you don't know what you have, you're going to struggle. You will really struggle with protecting that environment, being able to patch that environment, knowing where your vulnerabilities are, knowing your entire state is paramount security. People trust us as a company for security and we need to trust ourselves and be able to secure our own product in our own environment. So, with that, being able to search through millions of our clients, if needed, in order to find out what you have out there so you can secure it or shut it down, or make sure it's patched. See what vulnerabilities are out there. There's so much more than just discovering something and saying, "You have a server and its Server X, now I want to know all sorts of things about Server X, not just its presence. I can run some queries in order to find out: Are you patch? Do you have vulnerabilities to say, when Heartbleed came out and the WannaCry malware stuff? Now we can start seeing with our vulnerability footprint is. And that's important to us for security as well. Because if you can't protect yourself talking to another company, trust you to protect them.

Andy: You are able to use BMC Discovery to win with those high-profile things were around like you mentioned Heartbleed, WannaCry etc?

Greg: As soon as those things were revealed Zero Day, we started looking. And it's not just me, with the community out there, there's lots of people out there in the BMC community saying, "Hey, that's happened. How can we do this?" So, we trust and rely on a lot of the community knowledge as well as the technical support from BMC on this. So, you guys have some really good resources that contribute to the community. Because these guys have been using it day in and day out, and there they'll say, "Hey, this is a fast way that we could do this." Or even preemptively, "We know this is coming or we know that this is an issue and we've been looking at as well side by side with our client." Those kind of relationships there are invaluable. They really are. Because you guys have that, that inside tribal knowledge of how the product is built. And when you guys release some things to help, that just makes life easier. Because I can produce some list quite quickly with a query and say, "Hey, this is what our vulnerability exposure is that I'm seeing based on the last candidates and what we have." And inevitably, it happened a few times, where a group of people think that they have X number of vulnerabilities or X number servers and we can say, "Actually you have this."

Andy: Have you experienced where someone's come and said with a firm belief that they know what they've got and then you come along and prove them wrong?

Greg: I had a manager at one point, they were wondering about a particular piece of software that their team had assured them that they don't have any more. They removed everything because there was a potential vulnerability with it. And he came to me on the side and says, "Can you look?" I said, "Absolutely." So, I waited for the latest scan of the machines and said this is what you actually have. So, it may have been lying dormant. Maybe your guys just missed it because, you know, that's human error. They may not know everywhere to look, for patterns, in the deep, dark corners of something, to find it. And it was nice to reveal it. The one big thing with the Discovery solution from BMC is providence. Which, I told you that you have this, and this is why I told you, it's not just taking it on blind faith. You can actually go and look at the command that it ran. I've done that as well, I handed them off to people, "You go around this command manually to see what's out there."