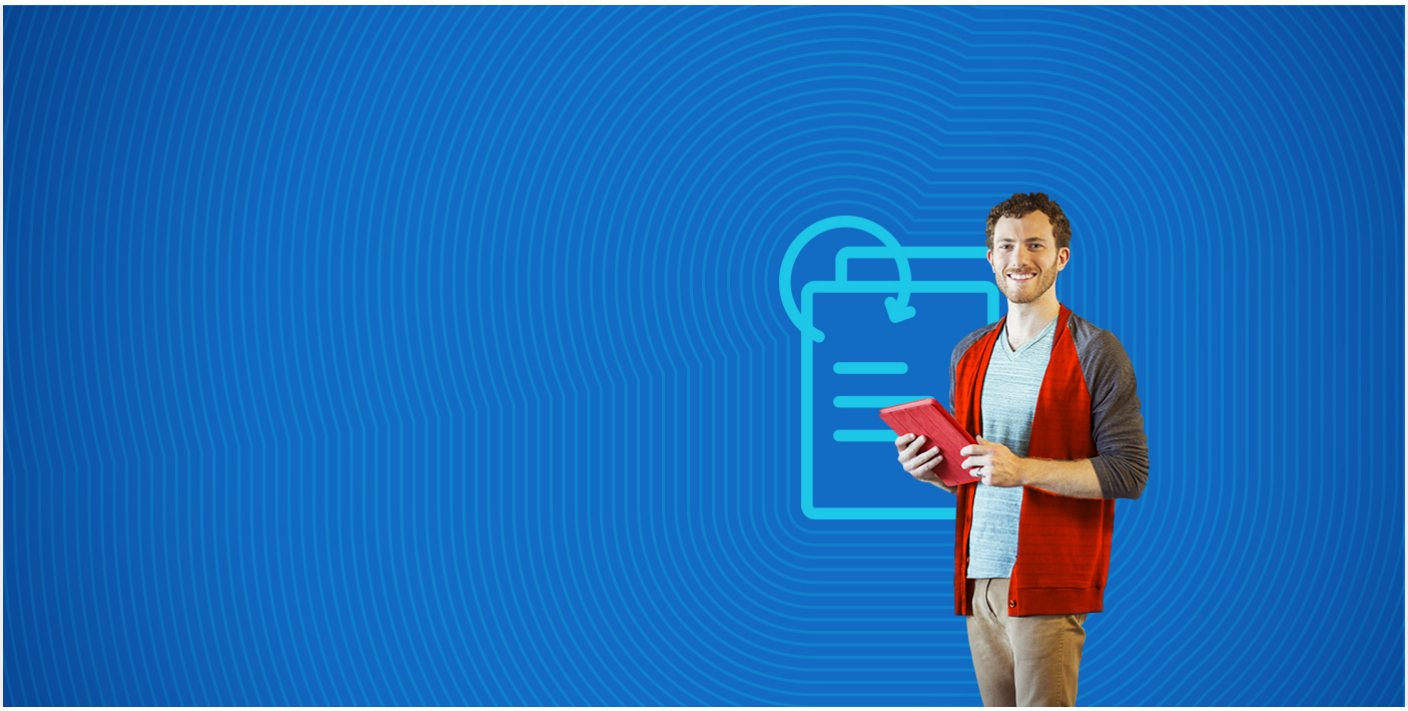
# WHAT IS XDR AND WHY SHOULD YOU CARE ABOUT IT?



BMC AMI Z Talk · Episode 2: What in the World is XDR and Why You Should Care about It

*In this episode of BMC AMI Z Talk, security talking heads Grant McDonald and Chris Perry from BMC chat about XDR, what it is, what it means for your business and why you should care about it. Below is a condensed transcript of our conversation.*

**Grant:** XDR is a term that is beginning to float around more and more. We have acronyms. We always have some hot new thing to chase after. And it's one Chris and I have been talking about as it relates to a lot of different technologies. Because as we talk with different customers, there's always a question about what's the strategy we need to be thinking about next? And that could be anything from XDR to do we need to factor it into our thinking?

So I think we should start with a definition. So, I'll give my definition, and Chris you tell me where you think I'm right or wrong on it. But as you look at it, I mean to break it down for those who are wondering what those letters stand for in XDR, it's 'extended detection and response.'

So, we've kind of had this EDR talk track out there in the info sec space for a long time. And it's kind of the idea that – well, we've looked at our endpoints. Sounds great, but we know the attack service is getting broader. We've got more devices being attached to our corporate networks. So, we need to look at everything. Not just our endpoints. But Chris tell me, what do you think? Do you agree? Disagree with that?

**Chris:** Yeah, I think you kind of hit it pretty well. You know I'm a product guy. Not as much a marketing guy. So, I usually laugh when I hear about the new buzzwords coming in vogue. But this one really makes sense. It's really EDR 2.0 where it takes a look at not just the endpoints, but network traffic analysis. And looks up to the security information of end monitoring systems. And it

brings it all together.

Because the truth is that when you were just having these disparate systems, it was a lot of data and context that was lost. Because a certain system would catch one thing, but we live in a pretty massively enterprise connected world. All these systems are touching together.

And so, if you weren't able to do detection or response across the entire extended enterprise, you really were missing some ability to develop some pretty high-fidelity indicators to compromise for what a malicious vector might be doing is they pivot from box to box in search of sensitive data. So, I kind of have a pretty good buy-in on it. I'm sold. I'll drink the Kool-Aid.

**Grant:** So, do you think – obviously it's an evolution, but I'm wondering what's the drive or the evolution? You mentioned context. I think context is definitely a big part of it. And trying to understand the journey of a potential attack on a company. But is it also just the visibility increasing of other things that are connected to the enterprise? And so, saying, "Woah. Didn't see that before. Better make sure we've got something in place to cover that, too."

**Chris:** Yeah. I think it's only that last one. When I speak with a lot of the security professionals at the big companies, it's really that last piece there. For the longest time it was the Windows computers being hacked. Maybe a Linux server was getting hacked. And so, a lot of the security, capabilities, and tools were built around defending those systems. It made the most sense.

But we're really seeing a dynamic change as every connected device is coming into play. I mean it was I think 2008 when Stuxnet, the US-Israeli virus, was able to take down a nuclear powerplant in Iran by going after the SCADA system. And you're a quick Google search away from YouTube videos of people hacking cars, hacking mainframes, hacking every system that would be connected on your network. So, when you think about that, you really have to take in all of these systems. Right?

You have to have all of that data connected there if you're going to see the lifecycle of the attacker's action. So, it's bringing everything together into one holistic system that is really what they're driving at here with this new buzzword. It's no longer just the Windows endpoints. Right? It's everything. Everything. One system. All the alerts tied together for actionable intelligence.

**Grant:** Yep. Yep. Good point. So, one of the other things that's obviously another kind of buzz or strategy term out there right now that I personally feel has some overlap is Zero Trust. Zero Trust has gained – it's not new. It's been around for a long time. But in the last couple years it feels like people have really started to grab onto it. And in my opinion, it's because of the same factors you just kind of outlined of all of these devices now kind of appearing more and more. At one time it was great to say you should trust – you should not trust anything until it's proven to be safe and secured.

But my belief is that kind of seeing different customers throughout both our world and just out in the social media world, that connected device platform just kind of attack service expanding. Now they're starting to say, "Okay. This idea that I need to not trust anything as secure until I've really taken a look at it has licks." So, I mean, do you think there's overlap there?