uberknowledge

# Ben Johnson, CTO and Co-Founder, Obsidian Security

## An Unusual Cybersecurity Creed

In a crowded security marketplace, Ben believes that people are happy to have multiple security tools but want fewer interfaces. He highlights the value of conversations with customers, points to the value of feedback, and shares his unusual corporate creed.

02:22 An unusual cybersecurity creed: Passion, Capacity, Humility.

06:02 The technology you're building needs to address a real problem. How does it fit into the tech stack, the workflow, the trends?

07:50 Everyone wants to be the dominant platform, so who should you choose to be your dashboard?

08:37 People are OK with multiple tools, they just want a very small number of interfaces.

09:08 Your customers will be different, so you have to build a product that is extensible and flexible to serve all of them.

10:34 Having conversations with your customers is always extremely valuable. Gather as much feedback as possible.

13:09 Privacy and security is different to privacy and ethics. The distinction is are you facing customers or are you facing your employees.

13:33 The frustration that led to regulations like GDPR was born out of consumers not knowing they were the product, but we all have a data price.

14:04 Employee privacy is a tricky issue. We have to find the balance allowing people to work without friction, but be able to stop them as soon as there is suspicion of insider threat.

16:00 Obsidian is about partnership and catching the bad guys.

Ashwin Krishnan: [00:00:46] With me today I have Ben Johnson from Obsidian. Now before we get into a lot of interesting topics, I actually picked up a few things from your LinkedIn profile which I have not seen any cybersecurity leader's profile. So we'll get to that in a minute, but before that can you give a little bit about your background for our listeners.

Ben Johnson: [00:01:06] Sure. So, I'm the CTO and Co-Founder of Obsidian Security. We're a Series B, early-stage company based in Southern California focused on identity, security, identity protection. I'm happy to go into that more detail. Previously I was fortunate enough to be the Co-Founder and CTO of Carbon Black, an endpoint security company. They're doing very well now. I have a lot of friends there, I wish them the best. And previously, I was NSA and intelligence community for seven years. So, a lot of just really fun security work on the classified side.

Ashwin Krishnan: [00:01:41] Cool. So, let's get into your LinkedIn profile and, I kid you not, I have not seen a profile that talks about belief in passion, capacity, and humility. Now these are not words that you see in a cybersecurity leader's profile, it's quite the opposite. What caused you to put this on there? Was there a wake-up call somewhere along the way or was it from day zero to where you are right now?

Ben Johnson: [00:02:10] Yes. So, first of all, really cool the approach you're taking, where you're trying to find interesting aspects to talk about and not just repetitive run-of-the-mill questions. So awesome.

[00:02:22] It honestly started in the intelligence community with a boss Paul Myrek who a lot of us really attribute to growing just an amazing team, an amazing culture. We were on this team called Intrusion Operations Division. So, if you just break that apart it's pretty interesting, and it was a lot of really hard-working, intelligent people coming together to solve national security missions and things like that. But it was his phrase, I don't know if he took it from somewhere else, but I think he put that together in the sense of that's what you need to look for when you build a team, when you hire people. And so, we thought about that enough where we repeated it, and it became this creed or saying. Then at Carbon Black we repeated the same thing, and then at Obsidian we're trying to embody that as well. You have to look for someone that really cares, and impassioned means you're willing to suffer for the cause, right? So hopefully, people are willing to suffer — if anyone is listening — for cybersecurity or for Obsidian or whatever. Capacity is not necessarily have you done this exact thing before, but do you have the capacity to do great work, do hard work, that kind of thing. And then humility is you're not a jerk, you're easy to work with — team first, low ego, that kind of thing. I really believe in that. I've written some articles that I think have gotten some good responses. But that's why that's on there because I truly believe it starts with people and it starts with whatever traits you want to look for. You get to pick the traits that you optimize for, and I think those are the three that I've seen successful.

Ashwin Krishnan: [00:04:01] So the opposite of that is glorified, you being a jerk — you being the high IQ, Mensa, put everybody else down. So, I just came from the show floor at RSA and you get lost in the noise. Even though what you're saying makes perfect logical sense — do the opposite, and the opposite is the right thing to do, and you will get noticed — why don't other cybersecurity companies, large, small, doesn't matter?

Ben Johnson: [00:04:33] Yeah, great, great area to talk about. I think, going back to talking about people like Steve Jobs and others, I think there's even quotes from them that talk about this, but what happens too often is people get excited about the tech that they're building, but it's very disconnected from the problem. And you know, I think Jobs himself even said, you got to start with the problem and work back to the technology.

[00:05:01] There's two groups that could use some benefit here. Too often it's either, I want to do something in cybersecurity, so I'm going to try to build something, but I don't quite have that knowledge that you're talking about. I haven't firsthand sat in a SOC or done instant response or done some pentesting, and so you're pretty disconnected from the actual users. The flip side of that is users come out of these three-letter agencies or other places, and they saw a very specific problem, but they don't maybe realize that problem is not a universal problem. So, it's a very niche or it's almost a feature not a full solution. And having said that, I think you can't discount how valuable customer conversations are. And if anyone that I've chatted with is listening, thank you, I truly appreciate customer conversations.

[00:06:02] But you know there's thinking about the whole end-to-end problem. If you're a buyer of technology, it's not the financial cost. That's part of it, but it's the training, the maintenance, the procurement process. I'm on the vendor side, and I'm going through some of these six-month procurement processes just to get to a trial! I know people on the other side of the table who have invested their own time in working with their procurement officers and risk officers and all these other things. So you have to think about that whole thing, and then you have to think about is the problem solving going to fit into the tech stack, fit into the workflows, fit into the trends? Because it will take you a couple of years to build something probably. And then finally, there is this notion that the vendor community and the security industry is all about proliferation, more, more, and more. The security community, so think about the weapons suppliers versus the soldiers, the security community wants consolidation. Ideally, they want one tool that solves everything. That's not possible, but they want fewer things that they can be really good at. And so how do we bridge that gap? I think that's something everyone's still trying to figure out.

Ashwin Krishnan: [00:07:12] So let's touch upon that topic. One of the things that was talked about at the CSA summit yesterday was just exactly what you're talking about. There's so many of these startups and large companies and then this thing about an API economy where things have to start talking to each other, so that there is this proliferation of platforms, if you like, so everybody is, hey talk to me. It doesn't matter how big or small you are, it's like, I'm going to integrate endpoint and network and cloud, etc. Do you see the bigger players starting to have a much stronger voice in this?

Ben Johnson: [00:07:50] Yes. The challenge is there is this notion of the really large players all trying to be the dominant platform. You could talk about the Workday and the ServiceNow, you could talk about Salesforce, Microsoft, Google, Amazon, all those players, but even companies like Slack, Dropbox, there's so many large players now where they're trying to pull in data. Actually, you even see this in banking. If I signed into one of my banks, it actually now has the capability to pull in my accounts from my other bank or my other credit cards. If I sign into my credit card thing, it can pull in my bank details. So, which one do I pick to be that that centralized view or dashboard?

[00:08:37] You mentioned the API economy. It is all about trying to centralize this view of risk or threats or just activity. And one thing we're finding is people are OK with multiple tools, they just want a very small number of interfaces. Like, sure I'll deploy 20 different monitoring detection tools, but I just want one or two or three areas to use it and use the information and take action. So, I think it's going back to some of that.

[00:09:08] The other thing is people need to build capabilities that are both easy to just plug in but also flexible. Like if you talked to a high-tech company up here, it's very different than a large manufacturing company in the Midwest and very different than a company in Dubai or something like that. So you have to, if you're a vendor, you have to build a product that's extensible and flexible enough to service all those customers. If you want to provide the returns that the VCs are looking for. So it's a very complicated equation about how you prioritize your roadmap and what you build.

Ashwin Krishnan: [00:09:44] On that last note, it's one thing to say you serve financials, healthcare, manufacturing, like you said, it's another to truly understand each of those verticals. In fact, this point was driven home in another conversation I had with somebody, and I was asking how does a vendor do this? They said something really simple: go to the conferences where your customer is going. If you cover manufacturing, have you ever gone to a manufacturing conference to see what their peers are saying, what challenges, what regulations? And it seems so obvious, but would you rather come to an RSA or a Black Hat as a security vendor or will you go to a manufacturing conference and then see the ROI of that? Are you seeing that sort of forward-looking thinking of let's not pretend that we understand the customer unless we truly dig in.

Ben Johnson: [00:10:34] Yeah. So, first of all just sitting down and having conversations with potential customers or partners is almost always extremely valuable. Unfortunately it's hard, their time is super limited and so getting in front of a CISO, a director of security, or whomever is challenging. I think you got to pick your battles and you got to focus on certain areas. However, the nice thing about cybersecurity is everyone has to worry about cybersecurity, so you can build solutions that are a little bit more universal or general.

[00:11:09] You can build this core tech that applies everywhere, and then it's almost like reskinning, new eyes, or having slightly different reports or slightly different integration points either ingest or output from a system into what healthcare is going to have versus high tech, telecom, or whatever. And so, it's finding that balance, and it is still really hard. But then, I do think going — to your point — to some of the conferences, you can't go to a lot of them but maybe if you're starting to get a lot of play in healthcare, you go to HIMSS or go to one of those conferences and really try to understand. But I think if nothing else, spend some time with some design partners, some customers that you're not looking to get revenue from for a while, you're just looking to learn from. And maybe they never become a customer, but you help provide value immediately you give them some expertise, give them some effort, and then they, hopefully, give you some good feedback.

Ashwin Krishnan: [00:12:07] So, going back to the topic of culture, I'm going to touch upon ethics, and you probably don't know, but I've had the pleasure of talking to Dr. Laura Noren. It was an interesting conversation because she talked about ethics, and she's obviously in your core team. It's one thing to get up on stage and talk about customer data and privacy and transparency and doing the right thing, it's another to follow that every single day, especially when your revenues are down, and customers are fleeing, and you have had a data breach.

[00:12:45] How does the industry come to terms with the fact that trust is at an all-time low? Talking about it, putting up banners about it is one thing, but if you know you had a data breach, do you come out and tell customers? So, do you see that cultural shift happening, just given the fact that you've been on the practitioner side as well as the vendor side?

Ben Johnson: [00:13:09] Yeah. You know, I think the challenge is there's a lot of focus on privacy and security versus privacy and ethics and it tries to be all wrapped up into one. But it's essentially two different groups between are you facing customers and consumers or you have employees.

[00:13:33] I think most of the frustration that led to things like GDPR was consumers not really realizing that they themselves were the product. And so, I do think there's a massive shift going on in terms of people being more careful about what they volunteer, what they give. But having said that, if you talk to just a random citizen, random person and this is a different country of course, but I think if they're getting enough value out of the platform then, you know, we all have our data price.

[00:14:04] From an employee perspective, it's trickier because basically when you sign up to work for a company or use an information system belonging to the government or you're a private entity or whatever, you essentially give up your rights to a lot of privacy because you're using their system. You're getting paid for that time. You're working on their intellectual property. But having said that, I do think we're trying to find a happy medium as a globe or a country around there being some rights for employees that every single letter they type on the keyboard isn't sent to some security team or something, but making sure that there's enough data available for a cybersecurity investigation or insider threat investigation, and that's where it gets really tricky. You know, I've heard people say we can't create friction for employees. They have to be able to move very fast, but as soon as there's any suspicion of either compromise or insider threat, friction goes out the window and we can stop them from working. It's finding that right line of continuous privacy versus security debate, but I do think there's some good progress being made. The pendulum is going to always be too far on one side or the other, but we just continue to adjust.

Ashwin Krishnan: [00:15:21] That's a great way of putting perspective on employees versus consumers and having a data price.

[00:15:29] So we are, I don't know, three blocks away from the show floor. It's nice and quiet over here. What would success look like for Ben Johnson at RSA2019?

Ben Johnson: [00:15:39] Just a handful of really good conversations that lead to the next round of conversations. I mean to be honest, I haven't been on the show floor and I probably won't even touch the show floor. You know, I've put my dues in, I've spent whole conferences on the show floor.

[00:16:00] We take the approach of let's have 20, 30, 40 really good meetings with partners, customers, etc. and really have a deep engagement and really try to listen as well as educate on where we see things going, what we see the value prop being of either our solution or just trends, and things to think about. So for me, it's really that our team has an enjoyable time and that the people we get time from feel like it was worthwhile to talk to us and then it leads to more conversations. We treat everything as a partnership and, you know, I'm fortunate that we treated customers well when I was at Carbon Black, and now they take my calls because we didn't just try to take money from them and run. We truly want to stop the bad guys too.

[00:16:50] So long story short, I just want have some good meetings, get out of here in one piece and get back to building product.

Ashwin Krishnan: [00:16:57] Very cool. This has been a really good conversation, hopefully the listeners will get as much value out of it as I did. Thanks for your time.

Ben Johnson: [00:17:04] Thank you.