Jason Brvenik, CEO, NSS Labs

Cybersecurity's watchdog

Jason offers an insight into the philosophy and work of NSS Labs. He discusses outdated dogma in cybersecurity, offers advice for vendors from large players to scrappy startups, and shares why he chose a career in cyber - he knew it was a domain that would never be mundane.

04:23 Vendors cover a spectrum of intents and interests; unfortunately, they are not always ethical.

06:46 How do NSS Labs maintain independence and impartiality?

11:37 Defence in depth — plurality does not equal better security.

14:20 Vendors do have an obligation to ensure they're delivering updatable, secure, maintained product within the lifespan

16:26 In virtualizing existing workloads in cloud environments we are lifting and shifting risk from a data center to the cloud.

19:19 NSS Labs have found they can use JavaScript to bypass protections in just about every next-generation firewall available.

23:11 Large vendors should really be offering protection, not just on one machine, but wherever the user is.

Ashwin Krishnan: [00:00:34] So, another edition of the UberKnowledge podcast. Today's guest, I'm going to have Jason Brvenik introduce himself. But Jason, I first met at Black Hat 2018, and he was at that point, I believe, the CTO of NSS Labs. But very recently, he's taken on the role as the head honcho at NSS Labs. So, Jason, why don't you introduce yourself to our listeners and we can get going.

Jason Brvenik: [00:01:01] All right. Hello all. My name's Jason Brvenik. Recently, the chief executive officer here at NSS Labs. I've been in the industry for quite some time and previously served as the chief technology officer here.

Ashwin Krishnan: [00:00:16] Excellent. Congrats first on your promotion to CEO of NSS Labs. I still recall our invigorating conversation from Black Hat last year. To just take it from where we left off last year, can you speak a little bit about what NSS is? What is it about? And then talk a little bit about how the overall independent third-party testing of security tools has evolved over the years and your prognosis of how this may evolve into the future.

Jason Brvenik: [00:01:49] Sure, NSS is a company that tests independently the capabilities of cybersecurity products, among other things. We perform these tests and produce our results in consumable reports that enterprises and consumers would read and understand generally how well their products are protecting them. What we then do is perform an analysis of the market and understand, by engaging with consumers, enterprises, government, states, and individuals at their home trying to select antivirus products, the things that drive their concerns, what they're most concerned about. We develop the methodologies in order to understand, can we test and assert a capability. We refined the methodology that we subject all the products that we test to the same criteria at the same time and produce these results. The value in this is that you can't actually as a consumer of a product, without attacking your own systems and attacking your own systems as an adversary would, tell whether or not it's working. We create the environment to safely do that, safely replicate attacker behavior, and to do it at scale that allows things to be comparable.

Ashwin Krishnan: [00:03:12] Great. Having been on the vendor side myself, dealing with NSS Labs is always one of those things. We really want to know how well or how poorly we are doing, yet at the same time, do we really? So, there's that yin and yang, if you will, of wanting to get a frank assessment of where one stands. At the same time, making sure that isn't something that the world gets to see until you have time to fix it.

[00:03:42] From your vantage position right now — I know you do private testing, and you do this public testing which everybody has access to — has there been a realization from the vendor community that truly figuring out what the holes are in the product and being able to actually address it helps elevate the entire conversation, makes the vendor whole as well as, more importantly, keeps the customer protected? Or is it still about, can I check the boxes and make sure I fit in the right place in the report that NSS Labs publishes?

Jason Brvenik: [00:04:23] You know, just like it is in society, there is a spectrum of personalities and interests and intents in cyber. I think it comes down to what's the real motivation. If the real motivation is to turn a profit, you tend to not see as much care about security and more checking the box. If the real motivation is the mission, much like what drives me, the mission to make sure that ordinary people don't have their things stolen from them by somebody they've never met or seen or considered even existed, you get a wholly different perspective. I think everybody, regardless of your motivation, should be interested in selling products and delivering top capabilities to the people that need them. In cyber, we're dealing with an environment where even our elections aren't safe from attackers. That you would sell a product knowingly or unwittingly because you didn't put the time in to understand whether or not it truly delivered on those claims, would be distressing to me. That being said, you know, there's a big difference between somebody that actually wants to field quality products, knows they're not there yet, but they do deliver good value and an organization that just wants to deliver features and sell products. That's really where I think the consumer needs to spend the most time assessing what kind of organization it really is.

> "In cyber, we're dealing with an environment where even our elections aren't safe from attackers."

Ashwin Krishnan: [00:05:54] Right. The other thing, I think we touched upon this when we met last, is the growing influence that NSS Labs has in the vendor selection process. If I'm an enterprise CISO, I actually look at the NSS report to figure out, who do I even invite to the party? So given your role now as the head of probably the number one security testing organization on the planet, how does Jason think of his role to maintain what I would consider to be impartiality, yet at the same time, you do work with vendors and you get paid for doing the private testing, etc., so how do you maintain your impartiality while realizing that whatever you publish ultimately ends up becoming, if not the standard, definitely one of the main criteria that is used by enterprises and service providers?

Jason Brvenik: [00:06:56] Let me start first with the public test. We do not get paid to do a public test. It is conducted independently against our published methodologies, and everybody is held to the same standard. We do offer the ability for organizations — any organization for that matter, not just vendors — to assess their relative security against the methodology, their capabilities against the methodology. And that's very useful for enterprises, for vendors, for general consumers in understanding not just the capabilities to select your product or delivering, but the opportunities they have to field better security for their stakeholders, more often than not, shareholders or employees or customers.

[00:07:40] In that regard, maintaining independence is very much a perspective as well as guidance. In so far as when we start a public test, it's tested against our methodology. As long as it's in the scope of the methodology, it's in bounds, the general in bounds question comes down to, can an attacker do it? All right, then it's in bounds, and we publish our results. We don't allow any influence over that. We take, of course, subjective suggestions from all of the constituents about what's important and interesting. But we ultimately make the determination on whether or not it's relevant and matters to the consumer. For example, you know, it's not uncommon to get a suggestion from a vendor, and it's funny because they don't even try and wear them craftily, "We don't have that feature yet, we prefer you not test it." [Laughs] Well, of course you would, but we are going to test it.

[00:08:41] It's a little bit different when you're dealing with technology, and while it notionally fits into a category of being the product being tested, its function is not focused on that, and so, it would be out of scope for that technology. There's a number of technologies that are interesting in that regard. You know, their marketing would suggest they fit in the category, but the actual implementation of the technology doesn't do what everybody thinks that market does, or it doesn't do it on its own, and so it wouldn't be a fit and would be disqualified.

[00:09:15] When it comes to privately testing for enterprises or consumers or vendors. You know, that is a focused engagement that looks to dig in. It's a competent exercise of the product in the security stack being fielded with the results provided publicly. I have a lot more latitude on how far we dig into something, whether or not we attempt to push really hard and break things or whether or not we just do a categorical representation of a public test.

> "Less desirable organizations might look at independent validation as danger."

Ashwin Krishnan: [00:09:44] Right.

Jason Brvenik: [00:09:45] In that regard, the good organizations know that bugs happen, and they know that they need to constantly validate their product and make sure that they're achieving their goals. They will often engage every release to make sure that they haven't introduced a new issue. Less desirable organizations might look at independent validation as danger. And it's not an unfair perspective, by the way, in so far as an organization focused on a feature velocity, delivering new features to customers, would only see a test that points out opportunities to improve the security being delivered as distracting from that mission. Not an unfair perspective, I would say, not a pure one, not the right one in our space, but understandable.

Ashwin Krishnan: [00:10:33] No, it's very true. And a lot of it is also, like you mentioned, based on the competitive environment. So, you can't absolve yourself completely from other vendors who may not have a higher bar. But at the same time, I think given the nature of what cybersecurity really is and how much it can impact lives and livelihoods, I think it's a different conversation.

[00:10:54] So switching gears a little bit, I'm referencing a CSO online article from two years ago where you had a very provocative title, "Confronting Dogma and Outsized Assumptions in Cybersecurity." And a few you called out would be, just talking about it from the audience perspective, defense in depth and what does that look like from an assumption or dogma perspective, or victims deserve it because they did not patch. So let me ask you this, what prompted you to write this article in the first place? Have you seen some of these baseline assumptions change, or do we keep adding more assumptions, even though we haven't validated any of them?

Jason Brvenik: [00:11:37] Dogma is a fascinating place in security to dig into it. Ten years ago, strong passwords were all the rage. You got to have strong passwords. And we created these systems that forced people to routinely change passwords, to make them stronger and stronger and stronger to a point where they became impossible to remember. This created variations of memorable passwords that passed the rules but were no more strong than the last ones that were there. They're actually easier because it extended a lifetime. You could hash and then crack and then take variations on it. That kind of dogma doesn't serve us well. The data to support these conclusions is often not substantiated well.

> "We should really be focused on defending an organization and the threats it's likely to face with appropriate tools."

[00:12:19] Let's take defense in depth as an example. I remember a decade ago, 15 years ago, there was a big push for defense in depth and highly secure organizations, if they didn't have firewalls from two competing vendors to play back-to-back, they weren't doing defense in depth. That doesn't actually give you depth. It gives you redundancy. The depth you're trying to hedge against is that a bug in one firewall does not manifest in another firewall. OK, fine. But the probability of those coming to play versus the probability of the firewall allowing by policy something to occur and the user doing the wrong thing are vastly out. We shouldn't be focused on redundant, differing vendor firewalls. We should really be focused on defending an organization and the threats it's likely to face with appropriate tools. The data doesn't tell us that having competing products serves you any better. The data doesn't tell us that having multiple competing products in the same product class serves you any better. It actually tells us it drives up your operational expense. It drives up your overhead. And it takes valuable, limited resources away from solving other, more solvable, higher-impact events and challenges. Until that would be the focus, I don't think anything's changed there at all.

Ashwin Krishnan: [00:13:46] There was another one that you had mentioned, which I found really interesting: vendors have an ethical responsibility to patch code that they might have spewed out 10 years ago. What's your view on that? I mean, I find that a really interesting conundrum. As a vendor, you have old versions of your code that have potentially been EOL'd that customers are still using. Do you still owe it to them and yourself to keep patching and keeping it up to date, or is it, been there, done that, EOL, so let's move on?

Jason Brvenik: [00:14:20] End-of-life is an interesting statement. Is end-of-life end of sale and support, etc.? I know enterprise environments that have applications that were written over 25 years ago that there is no vendor to go to get a patch for their applications. I do think that all vendors, all suppliers of software have an obligation to ensure they're delivering updatable, secure, maintained product within the lifespan, and the agreed lifespan of the product. Do they bear a burden? We can take this to an extreme. Somebody wrote software on a satellite; did this cross interstellar space, do they carry a burden to update the software on that satellite? Probably not. But if it's in wide-scale use and production use right now, you should patch it if it puts your users at risk, if you have the ability to do so.

Ashwin Krishnan: [00:15:22] That's a great practical way of looking at it. Depending on the impact, you should make that decision.

[00:15:30] So switching gears a little bit. I know historically NSS has been all about predominantly on-prem, hardware-centric testing — and some software-centric testing — but obviously, it's been about where the crown jewels were, which were typically in the data center on-prem. Now with hybrid cloud, multicloud, or all public cloud, how has the definition of what NSS Labs does changed as the move to public and hybrid happens? And number two, the velocity with which, let's say, security SaaS vendors coming out with a release every month versus once a year, how has that changed the dynamics in terms of how you and your organization have to evolve as well to ensure that your customer is aware of what's the latest and greatest and where some of the issues are?

"If it's in wide-scale use and production use right now, you should patch it."

Jason Brvenik: [00:16:26] Velocity is the right word. We've, because of the velocity, not just on the defender or the vendor side, but on the attacker side, created an environment that allows for continuous validation of capabilities. And continuous is every day, every minute, every hour. We can field newly discovered attacks or previous attacks against systems and see if they're still maintaining protections. We are in a world where operationally clicking on the wrong button in a product console can severely affect the security of an organization. We don't have the expertise to know the real details there. It's not like these systems say, if you do this, these things will happen, so continuous validation of your capabilities becomes pretty key there.

[00:17:15] On the cloud front, you know, that's an interesting domain, especially when we talk about hybrid clouds. Very few organizations that we've interacted with are capable of, in any near term, fielding cloud-native workloads. The vast majority of them are looking at virtualizing existing workloads in cloud environments and taking all of the issues and risks that exist in the existing environments and moving them into a new virtualized private container space in the cloud. The workload protections that are in place there matter significantly because you don't benefit from the cloud-based protections that come with cloud native. And I think we're going to see some interesting cases there. It certainly makes it more difficult to test because you have multiparty constituents involved. I don't think it makes it any different than if it were in your own personalized cloud environment.

Ashwin Krishnan [00:18:13] That's an interesting observation, you lift and shift risk from a data center to the cloud versus trying to refactor and go cloud native. That's definitely something worth thinking about.

[00:18:25] So one of the things that caught my attention, in your last answer was really the ability or the velocity of the bad guys. How do the people inside NSS, when you're trying to do the testing — it isn't typically like the QA testing a vendor does, you obviously have to think like a hacker and think like all the perpetrators who try to impinge upon the product and create vulnerabilities — so how do you guys keep up with, I don't know that it's a dark web, but just understand how the community works? Are there learnings that you have to keep up with within that community, so that you guys are thinking like the attackers versus how the defenders like to test their products?

Jason Brvenik: [00:19:19] Well, the good news is we've got tons of experience here. So we have the perspective of both. I have a small team who focuses on the offensive side of things that create new tooling and new techniques as an attacker would. That's their purpose. I have a team that then focuses on hearing the enterprises' threats and risk factors they are most concerned about. You bring the two together and you can field some pretty interesting capabilities.

[00:19:47] I'll give you an example from last year. Last year we tested a bunch of next-generation firewalls, as we've done many times before. In a technical sense, one would argue a next-generation firewall is supposed to protect its users from the internet. Users interact with the internet using browsers more often than not. And in a tactical sense, as a vendor, you would argue, well, the firewall can't effectively deliver security against script-based attacks and maintain an experience the user's willing to go with. Now, that's kind of a wordy response, but here's the simple statement: We found that we could use JavaScript to bypass protections in just about every next-generation firewall available. And it's not an unreasonable perspective to say the next-generation firewalls were never designed to handle script-based attacks. But it's also not unreasonable to recognize that the consumer of the next-generation firewall expects it not to recognize script-based attacks but to protect the user from the internet. And what that lends, well, it's hard to argue it shouldn't

“We found that we could use JavaScript to bypass protections in just about every next-generation firewall available.”

be at least attempting to do so in a robust way.

[00:21:01] And that's where the real divide comes in. You have millions of dollars spent on next-generation firewalls protecting users, and I got a small team of people that can create repeatable test cases; they can bypass those protections with reliability. Which leads me to the next one I love to hear, let's just say it's not an uncommon statement to hear, and there's two of my favorite phrases. The first one is, "Well, we don't see that in the wild, can we try something new?" And my first thought is, we don't see it in the lab either, so I'm not surprised. And the second one that often comes up is, "Evasions are one-off tricks and nobody cares." I find that to be a fascinating perspective insofar as, if I can bypass the protections with a one-off trick why can't the attackers? So, it goes back to the beginning of the conversation. The perspective you're dealing with is the most important one when you're selecting a partner to protect your organization.

Ashwin Krishnan: [00:22:11] Very, very true. So, I saved the best for last. Just brace yourself. This is not going to be easy, but I never said this was going to be easy. I want to put you on the spot because you have the vantage position. What's your advice to three categories of vendors? The first are the big ones who are getting bigger and bigger by the day. They're acquiring companies. They want to be this one-stop shop. Number two is plucky startups, which, obviously, are targeting a very singular, focused problem. And number three is infrastructure vendors who are adding security as an add-on feature just because they've finished compute, they've finished storage, and now let's go tackle security. From your perspective, what advice do you have for all three categories? What should they stop doing and what should they start doing - from Jason, the head of NSS Labs, talking to these three categories of vendors?

"Large vendors have large responsibilities, not just to shareholders, but to consumers and to society."

Jason Brvenik: [00:23:11] Great question. So, your first set was large vendors that keep getting bigger and bigger. You know, there's a number of things. The first of which is large vendors have large responsibilities, not just to shareholders, but to consumers and to society at large. I, for example, think that as a company, if I buy an endpoint technology to protect my company, really what I'm protecting are the users that make up my company. And a large vendor should really lean into offering protection to wherever the user exists. Not so much on the singular machine. I have a machine at work. I have a machine I use at home. I should never feel as a user like I need to forward something in my email from home to work because I think work has better security. We should have that kind of relationship well enough that I feel like work is extending their protection to home because I am part of work. And the vendor of that technology should encourage that work or that consumer to do that. That's one.

[00:24:09] Another is the large vendors focusing on the things that have the biggest impact is great, but ignoring the things that are entirely possible and targeted is not so great. Attempting, because you don't believe that the one-off trick is representative of the broader market, to avoid being validated and having independent validation, you know, that's kind of the raw emotion. You should lean in, give validation. If there's something you don't agree with, let's have a candid conversation about it and have a candid conversation with the market about it. It is incumbent upon you. As the market leader attempting to hide from it, that should give everybody concern.

[00:24:53] So your second was infrastructure players?

Ashwin Krishnan: [00:24:56] The second was startups focused on a singular problem.

Jason Brvenik: [00:25:02] Ooh, yes.

Ashwin Krishnan: [00:25:02] Again, given the defense in depth we talked about earlier, how can the CEO of a startup, how can she actually stand up and make herself heard when she's trying to solve a very, very focused problem?

Jason Brvenik: [00:25:15] Well, a very focused problem doesn't mean it's not an important problem and doesn't mean it's not a widespread problem. I'll discourage this much, claiming that you solve it 100%, that's just an invitation for your claims to be attacked. But demonstrating and challenging the market to see that it is a real problem and how you solve it is key. For example, you would look at next-generation firewalls, a pretty commodity-established market, but we see some pretty interesting players coming in and challenging incumbents there. There's no better way to get out to market and demonstrate the superiority of your approach to the one part of the problem, and being equal to or as capable as other products, than to lean forward and figure it out, demonstrate that, and demonstrate that through an independent engagement. If you're so narrowly focused that it's a point product that requires its own set of information, at that point, well, once you solve that problem, pivot pretty quickly. The market has lost a lot of tolerance for point products, best of breed products at this point and expects the larger portfolios to begin to offer them. Not an unreasonable perspective. Certainly, it can challenge the security perspective, but operationally, organizations don't have the wherewithal to maintain 80 point products.

“The market has lost a lot of tolerance for point products.”

Ashwin Krishnan [00:26:41] Got it. And infra players who are adding security as, not an afterthought, but something that they need to essentially complete their offering?

Jason Brvenik [00:26:53] Yeah, infrastructure players, it's interesting. You know, my mail provider just gets rid of spam for me. It gets rid of phishing for me. I don't have to pay for it. It's not a layer on top. It's just built in. I think as an infrastructure player, you know, the infrastructure is made up of the consumers and users of the infrastructure, and security needs to be built in from the start not added on later. Any infrastructure that isn't in its latest iterations or future iterations, failing to express not just the security they're offering, but the trust they're building in, I think is one you should challenge to have an evolved path too. I think trust is an interesting concept in our space in general, but being able to at least assert the approach you're taking to ensure that the infrastructure you're providing is doing what you intended it to do would be a great start.

Ashwin Krishnan: [00:27:50] Great answer. And finally, advice to the next generation of leaders? Whether it's Gen X, Gen Y, Gen Z, millennials, why would somebody consider a career in cybersecurity? What is Jason's advice? Let's say, two reasons why cybersecurity is a calling that they should at least give a hearing before jumping in or dismissing it.

Jason Brvenik: [00:28:22] Yeah. Well, I'll tell you why I chose cyber. Of all the information technology domains, it was the only one I estimated would never be mundane. It would never be so operationalized that it could be processed out as a product to checkbox a series of compliance checks. And that is because it's the only domain that will forever consistently face adversarial intent. Adversarial intent is what keeps it interesting and is what keeps me thinking about all the new ways to help solve problems and get better security. There's always a push. There's always something new. It's a fascinating domain. And ultimately, if you're into that kind of challenge, helping solve difficult problems in asymmetric issues, you should get into cyber.

"It's the only domain that will forever consistently face adversarial intent."

Ashwin Krishnan: [00:29:12] Great. I think that's wonderful advice. It's a problem worth solving. And like you said, it doesn't go away, unfortunately, even though we wish it would. The attack vectors and the methods of attack also keep changing, so it keeps life interesting.

[00:29:29] Jason, again, thank you for your time. I know we scheduled this at short notice, so I really appreciate it. Congratulations again on your promotion to be the CEO of NSS Labs. I'm looking forward to continuing the engagement in the future.

Jason Brvenik: [00:29:43] Thank you and have a great day.

Ashwin Krishnan: [00:29:44] Thanks.