THE PAYMENTS SHOW

http://thepayments.show

E86:
THE ROLE OF IP GEOLOCATION IN E-COMMERCE: MITIGATE ONLINE FRAUD, ENHANCE AD TARGETING PRECISION, OPTIMIZE CONTENT LOCALIZATION

GUEST

Jonathan Tomek

VP, R&D @ Digital Element

HOSTED BY

Satwant Phull

[Important]

- This transcript was produced with machine learning and has many ***errors and omissions***

- These timestamps are for the ***audio version*** of the podcast

[00:00:00] Start and Introduction

[00:00:00] **Satwant:** Hi, I'm your host Satwant, and welcome to this episode with Jonathan Tomek from Digital Element. If you'd like to watch the video version of this podcast, or get the PDF transcript, please either click the link in the show notes, or visit thepaymentsshow.substack.com. Enjoy the show..

[00:00:21] Jonathan, welcome to The Payments Show.

[00:00:24] **Jonathan:** Thank you for having me.

[00:00:26] **Satwant:** so Jonathan, you are the Vice President of Research and Development at Digital Elements, which is based in Georgia in the USA, and Digital Elements. is a company that helps businesses to understand more insights about their customers through their internet connection at a very basic level.

[00:00:44] And before we talk about that in more detail, I'm just going to give the audience a bit of your background. So you're an expert, you're an information security expert. Your background is in threat intelligence, network forensics, malware analysis, and. The whole gamut by the looks of things. You've had roles from everything as a security person at the U. S. Marine Corps, you've had multiple threat intelligence roles, and you've even founded your own hacking conference called ThotCon. So obviously a very highly technically capable person. So I'm sure you're, you've got some excellent war stories based on your career before we even begin, I think.

[00:01:21] **Jonathan:** Oh, there's, there's a lot. Yes, for sure. But, well we can go into a lot of different things as you want to. But yes, it's, it's been an adventurous time.

[00:01:31] VPN Stats And Their Implications

[00:01:31] **Satwant:** Sure. I always like to start off with an interesting stat. So Worldwide, it's estimated that 1. 6 billion people use VPNs I mean, I never estimated how many people use VPNs, but that's a lot higher than I would have guessed anyway.

[00:01:46] So I want to really start the conversation off to say, well, how is that relevant to somebody running an e commerce store and. What you guys do in the security space.

[00:01:56] **Jonathan:** Sure. So I'm going to say that even though that 1. 6 billion used that, it's not every single day because it's such a variety and that's just a really good estimate. Fraud markets even higher, like their percentages go much, much higher, but for what it's worth and why this is even relevant in a sense of e commerce is and we've seen this explicitly, especially in the airline industry, that you can purchase cheaper tickets based upon where you're located.

[00:02:27] You could even get different items bought in like a different country because you're able to get and circumvent different types of taxes if you can forge your location. So it's it can actually have business implications if you consider that too, because if you're going back to like the airline concept, if somebody is able to circumvent and start getting a hundred dollars off tickets and they do this all the time and other people catch on, this could start big developing to a bigger problem over time.

[00:02:55] **Satwant:** Sure. And then obviously, that affects the tax revenues and sales taxes around the world as well. Yeah, absolutely. Okay, great. So thanks for that background. I mean, there's so many things we can talk about in this space around why a customer's location is, is so critical. At the very basic level, if you're just on the internet and you connect to a website, that website provider can have some kind of add on or software that says where that person's from. And then obviously, a VPN, you can set your location to wherever you want. So my next question would be, okay, so if you know that they're not from there,

[00:03:31] **Jonathan:** hmm. Mm hmm.

[00:03:32] How Do You Find The True Location Of A VPN User?

[00:03:32] **Satwant:** how on earth do you figure that out? And what other information do you look at to provide the business owner with what they need to know to, whether to conduct that transaction or not?

[00:03:44] **Jonathan:** Great question. So based upon what you're saying, which is how do we figure out that somebody is using a VPN to circumvent restrictions? So one of those methods that we do is we actually just use the VPN! We figure out how these providers are offering their services and what services they offer.

[00:04:03] Because not every VPN is nefarious, for that matter of speaking. Not everybody is going to use it for fraud, etc. But they, a lot of people use it because they want to circumvent geo restrictions. So, that's the number one thing. We leverage and find as many different type of providers that exist out there so that we can actually monitor and see what's happening. So if we want to say, we're going to use VPN A and they allow you to come out very specifically in the center of London, which is an interesting element there too, because it lets you get very, very Precise in locations for some of them, so we'll check that out, and then we will dig into a little bit about like, who, who are they offering these services to, what are they trying to figure out, we, and then also what different regions they're allowing it to, so it's, it's all about figuring out what the big packages of the, these offerings, it's our goal is to figure out what they, I'm going to call it the integrity of an IP address so that we make sure that people are We're, we're helping users rather than hindering them because believe it or not, a lot more people as time goes on that use these services, don't really realize that they're actually hurting themselves over time when it comes to leveraging some of the services.

[00:05:19] Non-human Internet Traffic: Proxies

[00:05:19]

[00:05:22] **Satwant:** really interesting point that part of your solution addresses is non human traffic. So it'd be great if you can dig into that because I briefly read about things like proxies and darknets. So it'd be great for you to explain what that's about.

[00:05:39] **Jonathan:** Right, and so I apologize if I go down that rabbit hole a lot because that's something that I'm very passionate about because I like making sure the internet's a safe place of course. So the proxy part and the VPN part is they kind of go hand in hand and what really matters to the this whole ordeal is that's where I'm going to say a vast majority of all your fraud is going to come from.

[00:06:00] We're talking about credit card transactions that are trying to buy fraudulent things, et cetera. But they, there's so many of them, which is why it's become such a hot problem in the entire community because as soon as something is tested, they can go to the next one, the next one, next one. And so it's, yeah, it's, it's a big topic, so I think we can probably dig into that more if you had good questions about that. Mm

[00:06:29] **Satwant:** had some hope when virtual credit cards came into the mainstream. And I thought, Oh, this is great. You can. You can have a separate number for your online purchases and what have you. But I noticed for the first time personally when I tried to buy some software earlier this year, actually, no, it was a newsletter subscription.

[00:06:49] The virtual card was not allowed by, and I don't think the person who I was buying the newsletter from even knew this because they had a hosting provider. That allows them to sell their PDFs or whatever. I think that the way they had implemented Stripe was that you can't use virtual cards. So yeah, it seems that even though if there are solutions, there's challenges with those as well.

[00:07:10] **Jonathan:** Absolutely. It is. It's hard to know because there's, it's basically chaining of the events of different types of fraud. It's somebody could leverage a gift card and then bring that to Stripe or buy a virtual card and then bring that. And it just starts adding up and then you have this entire flow of fraud.

[00:07:29] That's why they, they basically went this draconian approach and cut it right down the line, which also limits your user base, believe it or not. Cause a lot of virtual cards are coming out now.

[00:07:41] **Satwant:** Yeah, I thought they were fantastic. And now I've had to flip back to using the plastic card, which makes me nervous online.

[00:07:47] **Jonathan:** Yeah.

[00:07:48]

[00:07:48] Additional IP Insights: Carrier Databases, Demographics and More

[00:07:48] **Satwant:** one part of your solution around additional IP insights. So. we know we're talking about location and trying to figure out where this person is, but let's talk about the intricacies about that. So things like mobile carrier databases. You've got things like demographics. You can determine the longitude and latitude. There's so many different areas. It'd be great for you to maybe pick on one or two, which are really great for e commerce businesses as an example.

[00:08:17] **Jonathan:** Sure. So this is, it's a great question because we have a lot of different types of data within our data sets that can be very valuable to people. Like you said, the demographic data, which could be something of interest to some people for sure. But when it comes to just the regions, I think that's, that's probably one of the more important things because you want to know what your target audience is.

[00:08:40] And then with that, it's being able to say, Hey, I need, which a lot of people know how the ad market works. You say, Hey, I want this to go to all of the UK. This is specific. But what if you wanted it to be in even more specific areas and then add additional types of context to it because you might care about it being in the UK, but what if you only cared about it for being somebody that had a specific like.

[00:09:08] A new, a new mother, for example, even though that's something that we wouldn't necessarily have that data. But what if that was something you were interested in? Some of the demographics would also be able to present that to you to give you a little bit more insight or even prevent somebody from forging those requests to say, Hey, I know that this is where all the money is.

[00:09:27] I'm going to funnel it right through this one spot. There's a lot of different unique insights that can be driven from just the IP addresses alone.

[00:09:35] **Satwant:** Yeah. I did see that, you know, a couple of the key benefits of businesses of your solutions are localized content and targeted advertising, along with things like digital rights management. And analytics and .

[00:09:46] IP Characteristics: Evolution of IP Addresses Over Time

[00:09:46] **Satwant:** You've also mentioned that you've got a new data set called IPC, not sure what that stands for, but it's, it's sort of the next level of your data set from what I can understand. Maybe you can perhaps expand on that.

[00:09:59] **Jonathan:** It's, it's an additional insight and it's what we're calling IP characteristics. And basically what it's doing is watching how IP addresses evolve over time. So for example, if your IP address is where you're saying it is right today, but what happens if it changes every day, all the time, you're not going to necessarily have the correct insight.

[00:10:23] Because nothing's static on the internet. Everything changes very dramatically. But with how we're collecting our data, we can say, wow, this IP address has been a school for this duration of time. If we see different types of actions coming from it, meaning like we can definitely say that this is, this is the company, this is the business.

[00:10:47] This is like I said, if it, if we could figure out it was a school, you could probably say this, and this is static. That's great. But what happens if you saw the opposite side, which is an IP address that just constantly is bouncing around? You're not going to necessarily know that that is a valuable like it could be potentially used for different types of fraud or, but maybe not, maybe it's, it's just, it doesn't give you the exact characteristics that you'd be looking for.

[00:11:15] So we can find that. And that's, what's really cool is knowing. Wow. Look at, look at how variety, like vast stuff changes. And then what data can you apply to it to give confidence in the data you're gleaning from it?

[00:11:30] TOR, Anonymity and the Darknet

[00:11:30] **Satwant:** So in that scenario, I'm trying to think why. Would an IP address legitimately change very often if it's not nefarious? So Tor, in case somebody listening doesn't know, that's a browser where you can browse anonymously, I think. But I don't know about how the IP addresses work there. I think they change every day, like you mentioned, but is there a legitimate case for that?

[00:11:53] **Jonathan:** So what's funny, I'm actually going to say it's the opposite of what you just said. So Tor doesn't really change frequently. Because they're, well, it's, I know that this is really fun to talk about because what TOR was designed to do is be, allow people to just be completely anonymous on the internet so that when you're leveraging the network and if you go outbound through it, like you can go, TOR has an inside network too, that's what we call the dark net.

[00:12:19] That's when you hear like the scary things in the world, the dark web, it's usually people referring to stuff with inside of TOR. But TOR also allows you to go through and exit, but, and you'll. It's practically impossible for most people to even figure out who is using and coming out of TOR, unless you know the TOR IP addresses.

[00:12:41] So that's why often businesses block them because there will be attackers that use it and leverage that network. Even though those I'm going to say are, I'm going to call them more semi static, which they don't change too frequently. But what I'm talking about when IP addresses can frequently jump and move, it's It's oftentimes going to be I'm going to say probably more residential type of IP addresses, like for example, people's homes.

[00:13:08] So if you reboot your home router, you're more than likely going to have a brand new IP address. I know that sounds funny, but it doesn't mean it's fraudulent. It doesn't mean it's nefarious, but what it can do though is it changes up how that demographic data is, but it also gives you a, window of where the IP address range could be.

[00:13:29] Some IP addresses only stay within like the UK, but what happens if that IP address shifted to every different country around the world? That's some of the insights that we can give you, which is. Wow. That IP address is something like we should block probably pretty soon. We're keeping track of all of those things because if you wanted to block all traffic from a country, like say that we didn't want to see anything from Russia, hypothetically, right? If an IP address that was in the UK now is in Russia and your list did not include that IP address in the Russian thing, you're now allowing it. See how that works? It's, it gets complicated, but it's, it's actually a really big problem for some people.

[00:14:12] **Satwant:** okay. That's really insightful.

[00:14:15] Customers Using Digital Element: Context Is key

[00:14:15] **Satwant:** if we look at the companies that you serve right now in terms of your customers, it's quite a broad range of advertising, broadcasting, financial services, social media platforms, online gambling. So I wanted to ask you two, two parts to a question. So are all sizes of business, small, medium, and large and enterprise businesses using your software. And the second part to the question is there's so many types of fraud, you know, card fraud, phishing, state sponsored. There's so many types and if certain ones of those are clustered with different sizes of business

[00:14:55] **Jonathan:** So the first part of your question, which was who's, what kind of business is leveraging our data? It is a variety. I will definitely say small to medium businesses are and very large businesses, but everybody uses our data differently, which I think is what's really powerful that I like to say that we are a perfect compliment for many different types of data sets.

[00:15:16] Because it's, it's context. We're, we're delivering something that any kind of platform can leverage, whether it's the geo parts of it, whether it's the integrity of the VP, if it's a VPN or a proxy. And it could be used by different parts of the organizations, which is why we're a lot of, I believe a lot of people can use us.

[00:15:38] Not that I'm trying to pitch our company at all, but I want it. I mean, it's actually a crucial part of a business. And. Like, when you think of the fraud departments, if they are trying to investigate a string of types of fraudulent activity, it helps to know where some of that's coming from. Not only to know, like, let's cluster this piece of data.

[00:16:01] They could glean that from our dataset, but also it helps you with the targeted advertising. It also helps you with other types of analytics that people probably don't even think about. So, so it's a good variety of businesses that use us for sure.

[00:16:14] **Satwant:** and for the smaller businesses. Are they using your solution indirectly? So for example, if they have a Shopify store, okay, that's a small business, but Shopify is a huge business. Is that how that typically works or do they come to you if they need help?

[00:16:32] **Jonathan:** So a company would be using our data. So Shopify would be using our data to help them with their side. And so indirectly, I would say that most people around the world are probably using our data without ever even realizing it on a day to day business day to day event. But yes, if Shopify would be the primary user here to help them with knowing what kind of Data insights they would need.

[00:16:56] But in addition, like if a customer was using it, they potentially could say, Hey, I'm Shopify saying I'm over here. Why is that? That's the case. It's probably because they're not using our data then. But anyway, it's a lot of people can use it in different ways. Wow.

[00:17:13] **Satwant:** it's a very rich data set because your company's been going since 1999 and I think I first used the internet. Would have been around 94, I think. I think it was in Florida if I remember. My parents took us all to Disney World and I think in Epcot, they were showing the internet. I think it was AOL.

[00:17:35] I think they'd set up some PCs. So, geez, that's a long time ago. And I was just amazed. I was hooked from that point. So there's a very, very long history you've got there.

[00:17:47] **Jonathan:** Yeah, it's I actually started with the internet very early, just like you have. I grew up with it because my mother got very early into the big e commerce space, the dot com boom. But yeah, that's, and so that started me down that path. Cause it's a lot of fun. The internet's a huge thing and it literally tied everything together.

[00:18:06] And it's actually kind of fun knowing. How so many people said it would only be very short lived and now look at it, tied everything together.

[00:18:15] **Satwant:** Yeah, absolutely. So, based on that, I guess you operate in countries all over the world in terms of your offices and where your staff are, or is it concentrated in North America?

[00:18:26] **Jonathan:** We're primarily concentrated in North America in several different places, but our headquarters is in Atlanta, Georgia, for sure. We do have offices around the world for sure too. I think the beauty of our business though is we're agnostic. Like, it doesn't matter where we're located because we do the entire globe.

[00:18:45] **Satwant:** Great stuff.

[00:18:46] Overview of the Solution

[00:18:46] **Satwant:** I want to move into talking about your solution. It's kind of split into three major parts. So you've got something called net acuity, which is for your location targeting, you've got threat intelligence, which covers the proxy and VPN that you mentioned earlier. And then you've got like another banner, which covers additional IP insights.

[00:19:06] So, so those are the main three areas. And it'd be good to know when a company engages with you first of all, how, how does that happen? What does, what does the length of that engagement look like before they typically go live with your solution? And, what kind of setup do you typically have for customers or is it very customized?

[00:19:25] **Jonathan:** So that's a big, broad question because we, we like to work with the customers the way that they need it to. And based upon the solutions that they're going to need I mean, we like to give everybody a bit of everything because for what it's worth this is why I like to call it more of that IP integrity concept.

[00:19:43] It's that insight of the data because not just that. The geographic region matters. But what happens if you have, you're located very specifically in the U. S. and you only care about U. S. centric things. But if customers are leveraging VPNs and proxies and forging their location, that would also affect you as well.

[00:20:03] So it's kind of a What fits you and what do you need sort of solution? So, and we can explain how all the different use cases would apply to you. Cause when it comes to like DRM use cases, right. Or ad advertising, there's so many different use cases. So we would definitely be able to explain how that all works.

[00:20:23] That's, that's a crucial part of it too. But the second part sorry, can you fill me in? What was the second part of your question? Just cause I want to make sure I answer correctly.

[00:20:31] **Satwant:** Yeah you've got three main areas of your solution. how long does it typically take to implement with a customer?

[00:20:39] **Jonathan:** So that's, and that's a great question too because we, we have different types of methods for customers to integrate with our product really quickly. So we have an eight, like a RESTful API, like the, the technical terms that I could probably leave out of here, but we offer different methods for any kind of customer to leverage really quickly.

[00:21:00] And it shouldn't take too long. I mean, it's we've been doing this for many years, of course. So any customer that comes to us where we get them up pretty quickly.

[00:21:11] Strict Payment Processing Rules Don't Solve All problems

[00:21:11] **Satwant:** One thing I wanted to ask, a relatively straightforward way that businesses can determine where you are, if you're going to. And I saw this when I first set up a side hustle a few years back, I had to open a Stripe account. And one of the things you have to do in there is set up various levels of checks that you can choose.

[00:21:30] So for example, it would ask you, do you really want to check the billing address or you're not that bothered? And there was various levels higher than that as well. Do you want them to verify with an SMS or it was different levels. So. Could businesses just save themselves a lot of headache if they simply knew, because I'm assuming they don't, if they simply knew that they could do these kinds of things?

[00:21:55] And one example that comes to mind is selling cannabis in the states, because states have different rules versus federal rules. That's one straightforward way where you could say, well, anyone around the world can check out our store, but when they come to buy, we have to have The Strictest Payment Checks.

[00:22:12] **Jonathan:** Absolutely. It's, there's, and there's a lot of reasons for why you would want to have a lot of, a lot more checks. I mean, letting anybody visit a site, I would say is probably not as big of an issue because there's even research and people that need to have access to things like that. But you brought up a good point, which is having additional checks, because let's hypothetically say that you were going to go purchase cannabis in the UK and you wanted to send it to you.

[00:22:40] Obviously there's legality associated with that. Even in the U S we have that with across different States. Like you cannot buy it in certain States, but if you allowed it as a business, you now potentially could have repercussions yourself because you now did something that you shouldn't have done. So your, your hand is kind of forced, but what happens if somebody was able to circumvent certain restrictions and they said, Hey, I can buy it because I am in the exact location, I have the right information to look like I'm in the spot that's allowing it, right? You used a VPN, you had the right GeoIP address, all these things, but then the mailing address was totally different. You now also would have a different level of, well, what do I do?

[00:23:26] This could also affect tariffs. This can affect different types of taxes because you now gave a product for whether it's illegal or not. Let's say it was something that wasn't illegal. You now are sending a product to a different country. That's going to be taxed at a higher rate and you gave it to him for a lower. So you ended up losing money on the whole business on the transaction.

[00:23:49] **Satwant:** Okay. See why it's a minefield now.

[00:23:51] **Jonathan:** Yes, it is a big problem.

[00:23:54] **Satwant:** yeah. I think I think that's the reason why some of cannabis shops in the States, I think they deal with a lot of cash because it just makes it easier if you have to be there physically.

[00:24:02] **Jonathan:** Yep, that is correct.

[00:24:04] **Satwant:** Great stuff. Okay. Is there anything important that you wanted to get across in terms of the sales side and helping businesses convert more easily that maybe I've missed something important that you want to get across?

[00:24:16] Next Steps: Getting Started with Digital Element

[00:24:16] **Jonathan:** If I had to say anything the, the integration piece is probably the most intimidating part for a lot of businesses to make sure that they're up and running and using, utilizing the data properly. But it's, I can say that it's very, I would like to bring comfort to people if they ever wanted to try it, that it's actually a really simple thing to do.

[00:24:37] And then we can also show you how granular some of these things can happen and or the data is, which also is another really crucial element to this because I like to say our accuracy is incredibly high, but we also offer another kind of dimension that if somebody was looking into it, which is that granularity.

[00:24:57] Down to like postal codes because some people care about that 'cause. So yeah, it can be intimidating, but just the the offering itself it's, it's really cool.

[00:25:07] **Satwant:** Yeah. So your website for anyone listening is digitalelement.com in case anybody wants to check out those solutions. So we'll move on to talk about some topical things, I think.

[00:25:17] New Threats: Connected TV Ad Fraud and Bots

[00:25:17] **Satwant:** Predictions for 2024, your company has highlighted the CTV space. And I didn't know this stood for connected TV. What's going on there and why is it going to be a big trend for this year?

[00:25:32] **Jonathan:** Wow. So in the CTV space, because that is a big, big thing that's coming up right now. There's everybody has a connected television now, whether you know it or not. If you think about it, whenever you go to a restaurant, half of those televisions are all connected to the internet. Even your one, it's all smart devices, IOT devices for that matter of speaking.

[00:25:52] But when it comes to all of the different types of trends, that's also where some of the fraud is also coming from because There's so many new types of devices coming online. I mean, we're talking, how many would you have expected to have in your home? Probably 20, 30 different types of internet connected devices in your house without even like knowing about it.

[00:26:15] **Satwant:** Definitely not.

[00:26:17] **Jonathan:** Yeah, that's, so that's, that's a, it's a big, big thing. So that's why there's And in addition to that, not many people even update those devices. So that's why there's going to be a really big push to combat a lot of the fraud that's behind that and securing some of those devices. But the, the ad fraud behind the CTV stuff is just so, so big.

[00:26:38] That's where a lot of bots are now coming from. And to give you an understanding why, D. Yes, people use a smart web browser on their television, but you're not going to be doing a lot of your internet traffic on a TV. It's not an easy thing to do. You have a computer for all those purposes. But a lot of these televisions are now being, or not just televisions in general, but just like the connected devices in general are being used to pivot and be, whether it's the IP address themselves of that device, or.

[00:27:15] The device it's, it's being used to create internet traffic and actors are leveraging them. I could have probably said that a little better, but it's, it's a big, big thing.

[00:27:25] **Satwant:** So I'm just trying to set the scene simply for the TV example. So it would be somebody trying to screw over a competitor and drain their funds. Is that right?

[00:27:35] **Jonathan:** That could be an, that's an absolutely a use case. Yes, for sure. That's one of the many, but the biggest part about it is the fact that there are so many devices around the world that all of those could be, could look like they're unique people. So what would you, here, let me throw this question at you, because this is probably one that's good for the audience.

[00:27:57] What do you think you'd be able to do if you had a hundred million IP addresses and you could look like you're a unique person, a hundred million people around the world, what could you do? That's a really good story. And that's what we're trying to help prevent and also figure out so that people have comfort.

[00:28:19] Mm

[00:28:21] **Satwant:** level. I was,

[00:28:22] Threats From IoT Devices

[00:28:22] **Satwant:** I've only thought about devices in my house on the first level. So I bought a dishwasher, a few. A few years ago, Bosch won, and it was an internet connected dishwasher. And I thought, could this thing possibly do? So I don't like putting IOD devices on my home network, but I connected it just to see what it would do.

[00:28:42] And all it does is it, when the dishwasher program is finished, the app tells you that it's finished. So I didn't think that that was a worthwhile security risk to have that thing on the home network.

[00:28:54] **Jonathan:** It's truly, it's not for a lot of people. That's not a, like, you have a firewall that's protecting it. You are very secure, and I'm sure within the past day or two, or you're going to hear it within the next week, that you heard there's three million smart toothbrushes out there doing distributed denial of service attacks around the world.

[00:29:12] That, no, no, that's not just That's not a real thing. I'm just going to straight up tell you that it's, it's very safe. There is a what if, because the, the powerful part and why this is, why this can be more concerning is it's not necessarily the appliance. I mean, yes, you should always update everything whenever you can.

[00:29:35] And yes, you can feel safe to plug these things in. It's, it's the people that. We'll like to buy some technology that's so smart that they're not going to use it and never update it. And then now it becomes a potential vulnerability because there's, it's, it's usually going to be like the app on your phone that you have because your phone is also part of this.

[00:29:59] of the internet connected devices. And then you also start installing additional plugins on your like set top boxes. You can't really do that with a smart dishwasher. So feel a little bit more comfortable there, but your smart refrigerator that you can do it to, that's a little bit different. So that's to give you a little bit more insight into the challenges.

[00:30:19] Yeah.

[00:30:26] **Satwant:** up on current threats, nation states, you know, China, there was an article recently that the US government's disrupting a botnet from a hacking group there and that's attacking US infrastructure like power plants.

[00:30:41] And then Microsoft and Hewlett Packard Enterprises has been attacked recently. So nation state style attacks are happening all the time now. And only, I guess only a small, tiny fraction make it into the news.

[00:30:55] **Jonathan:** Absolutely. You, and sometimes they're, whether or not they're bigger or smaller than they really are, it's very hard to gauge because the attack interface, like the, what you're looking at, you have to really tie all that data together and it can be very difficult. But all of these things are tied together because what nation states are doing is not much different than what the cyber criminals are doing. That's why I bring up the proxy part, because there are a tremendous amount of, in this case, like whether it's the set top boxes, which can be used for fraud proxies, which are Compromised home routers, which it's always a good thing every week or two, you know, just reboot your home router because that will get rid of any risks that you might have.

[00:31:41] Believe it or not, it's kind of a funny little thing that people don't think about, or just updating your web browser. But When you have millions upon millions of these connected always on devices that can be used by attackers, that's why these risks are getting bigger because we, we already know a lot of the if it looks like a duck, walks like a duck, acts like a duck, it's probably a duck.

[00:32:05] The bad guys know the same thing. So they're going to do everything in their power to start looking and acting and talking. It's, it's about time now that we started adding additional levels of context, which would be, Hey, maybe we need a DNA check at this point, but I don't know, I'm not saying going down the rabbit hole, but but adding additional context to what you already have, which could then say, Oh, wait a minute.

[00:32:30] Not only is that. It looks like a duck, but for whatever reason, that doesn't smell any bit like a duck. Why, why is that? You know, that's not a big deal. Proxies are a huge part of this factor because at any given time of the day, and this is something really important that we do. Because there's a lot of different types of services out there that say, Hey, we block proxies, or we, we can tell you what they are.

[00:32:53] We, we actually go really deep into discerning the difference between different types of proxies by giving you not just the name, but like what services they even offer. If this is of interest to you, like it might not be of interest to a bunch of people, but to the fraud teams, it can be huge. But in addition to that, we also do timestamps, which is It's massive because just because it's a proxy today doesn't mean it'll be a proxy tomorrow.

[00:33:19] Doesn't mean it was a proxy two weeks ago and doesn't mean the proxy from two weeks ago is relevant today. So we offer all of that and make it really to help you discern what's good and bad. So yeah,

[00:33:32] **Satwant:** and there were great tools in the platform that companies could use to set up alerts, but then third party software companies started popping up to say, here's a dashboard because it's overwhelming because it alerts you to everything that could possibly be wrong, which is overwhelming to anyone.

[00:33:48] So you guys have dashboards and things to make it more consumable.

[00:33:53] **Jonathan:** We integrate with all of them. That's what makes us really powerful so that you have less. Because that's the number one thing right now, which the goal is to reduce your costs and not increment your costs. I always think, especially your time, time is your number one thing because there's a million and one alerts that exist out there.

[00:34:09] But if we integrate with any of the tools that you already have, I mean, then now it's a time saver, which is big. At least it's big in my book. And then if it helps you make a decision more rapidly, that's also another time saver. So there's, that's why I like to call it the win win solutions when you start incrementing that way.

[00:34:27] **Satwant:** I did want to finish on that actually is the costs of your solution. How do you charge? What's your sort of business model? And just from a selfish point of view, I love investing. So are you a public company?

[00:34:38] **Jonathan:** Well, we're a private company right now, but at least to my knowledge, I don't know what the plan is, I know we definitely do annual licensing and that's always going to give you your best savings, et cetera.

[00:34:46] **Satwant:** yeah, yeah. Excellent. Good stuff.

[00:34:49] **Jonathan:** buy us, buy us for 10 years and you have the best pricing ever.

[00:34:52] **Satwant:** yeah, yeah, absolutely. No, excellent. Well, thanks so much for that. That was so insightful. I know this conversation could go on for another five hours, but I just wanted to make sure that I touched on various points lightly for the audience in case they want to dig deeper, they can go to your website

[00:35:06] which again is digitalelement.com.

[00:35:09] Chit Chat

[00:35:09] **Satwant:** And I'd love to finish the show with one or two light questions. So with you, I'm going to ask you for your favorite movie, I think today.

[00:35:19] **Jonathan:** Ooh, favorite movie. Okay. So. We, we were talking about a lot about fraud or just. And the craziness of what the money and markets are. I think, have you ever seen The Usual Suspects?

[00:35:35] **Satwant:** Yes. I have an interesting story about that. The first time I watched it, it was quite young and I hated it. And I was quite tired. I don't even think I got in more than a quarter of the way through it. And then I watched it about five years ago and thought it was one of the best movies ever made.

[00:35:49] **Jonathan:** it's, it's one of those movies that you're expecting. You want to know the outcome and then you really, it just twists and it's, that's one of my favorites. I have to say, yeah.

[00:36:02] **Satwant:** You maybe want to watch it again now. I think I

[00:36:04] **Jonathan:** Oh, I do. It's such a good one. We both do it together. We'll keep each other accountable.

[00:36:08] **Satwant:** Yep. I like it. Excellent stuff. Okay, great. Well, thank you so much. I really appreciate your time, Jonathan.

[00:36:15] THOTCON Hacking Conference, Chicago

[00:36:15] **Satwant:** And I think very lastly, it would be good to mention if people want to meet your company, Digital Element and maybe you might even want to mention your hacking conference, if that's still going.

[00:36:26] **Jonathan:** Oh, yeah. It's called ThoughtCon, so it stands for 312 Con, and it's based out of Chicago. And we're actually not having it this year. We're going to do it next year. It will be our 13th year. And it's a lot of really great insights. That's thotcon. org, T H O T C O N. org. And it's very educational.

[00:36:47] It's one of the most, I personally say it's my favorite conference, of course, but definitely check that out. If you're at any bit interested in tech.

[00:36:56] **Satwant:** Fantastic. And that's not, but that's not affiliated to your company or it is?

[00:37:01] **Jonathan:** It's, it's not, it's not, but my company does like to go there. And so we like to show our presence because we are invested in the community. So.

[00:37:09] **Satwant:** Excellent. Thank you so much. Brilliant stuff. Thanks and all the best to you in the future.

[00:37:15] **Jonathan:** Thank you. It was a pleasure being here and getting to speak with you. This has been great.

[00:37:19] **Satwant:** Cheers.

[00:37:20] **Jonathan:** Cheers.