RT: For today's episode, I'm joined by Kevin Lancaster, CEO of ID Agent, which is a name I'm hearing a lot about lately. At literally every event I've been to people have been talking about ID Agent and you've definitely got a buzz around you.

For anybody who's unfamiliar with ID Agent, how would you explain who you are and what you do?

KL: It's great to have a solution or platform that generates this much buzz and having this much impact. Essentially, we built this ID Agent platform, although the tool itself is called Dark Web ID, to help our MSP (managed service provider) partners really convey in very simplistic ways how bad it is out there.

By 'bad' I mean how bad the cybersecurity challenge is. Our tool shows compromised email addresses and passwords that we're finding out on the dark web, we can at times disclose other PIIs (personally identifiable information): mother's maiden names, credit information, last names, date of birth, that type of stuff.

We've had a quick emergence into this channel space after a couple of years supporting enterprise, such as government agencies, the largest banks and financial firms across the globe.

In this space, it's really had a significant impact on helping MSPs convey that cybersecurity challenge, when you can show somebody their compromised email addresses and passwords and show how many there are within the organisation. It really helps our partners get into prospects or go to their existing customers and really sell all the security solutions that they should be buying from them.

There's a lot of noise out there, and unfortunately, they get this concept of breach fatigue and people don't really want to kind of pay attention to it until something bad happens, until they're compromised.

That's one of the reasons why we had such a strong buzz or wave of excitement across the globe, because we're having that material impact, showing these compromised credentials and helping our partners grow.

RT: I work with a number of MSPs, and when I can usually tell there's an indicator that a tool or a vendor is going to do really, really well when the most progressive MSPs that I come across, start talking excitedly about a product. That's what's happened with ID Agent.

The MSPs that I've spoken to spoken to have said that it's really given them a foot in the door to start having conversations with prospects. But in practical terms, what does the tool do? How does it give MSP that foot in the door?

KL: Up to this point, has been hard for MSPs to get into a new prospect, show their capabilities and differentiate from others that might already be in there or knocking on the door of that particular prospect.
We built two sides of our application, the dark web tool. The first one is that you can run any domain, across the globe, for any organisation, and we'll show whether we have hits on that domain. If that email address or that domain has been compromised and we have a hit, that MSP partner can go in and show that there are records out there, their credentials out there.

Unfortunately, it's an overused term, but it does fit it: it's kind of a shock and awe tactic, because most people don't think about compromise and don't want to invest in security until something has happened. That's kind of par for the course.

The MSP can use this tool and show that business owner their compromised email address or show the fact that they've got 10, 15, 20 or 30 of their employees being compromised.

The feedback that we're getting from our partners is that it's having a tremendous impact on their ability to get into an organisation, and we'll quickly demonstrate they need to work with a particular MSP because they're progressive and taking cybersecurity to the forefront of the conversation.

This is better than saying, 'Let me manage your hosted exchange and your email.' They say, 'Let's start the conversation with security and let me show you why. The password that you use across everything you log into in the business and in your personal life is out there already, so you need to start with security.' This has become the visceral, high-impact solution that MSPs need to get in there and convey that message upfront.

RT: That totally makes sense. I want to talk about the tool later on, but before we get any further, we've referred to it - the dark web - what is it and how would you explain it to people?

Not necessarily to MSPs, there's going to be some MSPs listening who have heard that term, but perhaps don't really understand what it is. How would you explain what the dark web is to end users?

KL: Let's break it down in a couple of couple different levels. Every day, everybody uses either Chrome or Mozilla Firefox to do a search. They'll go out there and type in an address of a business that they want to check out or a site that they want to go shopping on.

At that point, they're putting in a URL, it's going out to an IP address, and returning a result. In a nutshell, that's the surface web, the web that everybody is used to using on a on a daily basis.

There's the surface web, and then there's a sub-layer, if you will, to that surface web. And that has been considered the 'deep web'. You don't necessarily put in a URL or a typical IP address, it doesn't end in a.com, or.net or a.org.

Oftentimes, it'll end in a .onion, so it's a different protocol. Think about the deep web as a layer beneath the surface web. We've got the surface web that everybody uses and then you've got the deep. Because of how the deep web was architected, and because it's an area that's encrypted, it's easy to be anonymous.
Smart, enterprising, and unfortunately less than savoury individuals figured out that they can carve out little areas or pockets, now known as the dark web, to do nefarious things. They could post pornography, they could buy and sell drugs, you name it. Guns, anything that you could think of anything that an enterprising criminal mind wants to sell, they go to that area of the deep web and create an anonymous site and start transacting.

That's how we coined the phrase 'dark web'. It's a sub-layer, it's not an area that it's easily accessible and most people don't know about it. When you add in the encryption protocols, the ability to anonymise yourself, you can see how it quickly becomes dark and mysterious and a place where bad things happen.

There're some good and valid uses of the deep web, but then there's this area of the dark web is just where all of those bad things that you hear about occur. That's where we look for data, that's where we look to see if we can extract credentials that might be up for sale.

If we can monitor and pull in that data, and then report to our partners that the data is out there, the mission that we're on is trying to find that data in the dark web, bring it to the surface, so that way our partners can show their customers or prospects that the data is out there and they need to take security seriously.

RT: I can see how valuable that would be. Given its nature, and without giving away any of your trade secrets here, how do you actually gather that dark web intelligence?

The way you've described it to me, it’s like a dark alley or a dodgy bar or, a place where there’s information perhaps from people that you wouldn't want to bump into. How do you go around and gather that dark web intelligence?

KL: That’s a question we get quite often. We've developed capabilities over the last 10 years, and a lot of our background has come from supporting government agencies here in the States.

A lot of the stuff we did with governments as a whole, and in some states was supporting them and providing intelligence. It is a moving target and it’s a seedy and shady area, so you have to be careful about how you go about trying to find data and what data you surface and report on.

It's a combination of individuals, human intelligence, going out and trying to figure out where's it going to pop up next, what is the next form, the next site or place where you can expect this data is going to be bought or published for sale, trade or exploit.

There are some technologies in the backend that, once you identify certain areas and you start monitoring, you can extract and scrape that data. It's a combination of both using the human intelligence, which really provides the high value data that we collect, and then using some of the automated tools that we can use to the descrip and extract different data that's out there.

The hard part is that there's so much data out there, it's such a moving target. These are enterprising individuals and organisations, and sometimes you'll come across data that might not actually be real, it might be fictitious or fake data.

There's a lot of care that goes into looking at what data we're pulling in and reporting. If we pulled in and reported on everything, we would actually overwhelm everybody, because of just the volume of data that it's out there.

There's a lot of care and trying to figure out if it is legitimate data, looking at the profiles of the hackers and individuals that are posting this data. Are they reputable within that underground marketplace and have they been successful at selling legitimate data in the past?

There's a lot of care that goes into making sure that we're reporting on data that's not fictitious or false positive data and putting it in the platform. Not sure if that gives you a direct or indirect answer! In short, it's a combination of human and artificial intelligence that we use to extract data out there on the dark web.

RT: At the end of the day, you're doing the hard work, you're providing the data, perhaps about MSPs’ clients or prospective clients. Let's talk about clients first of all - are you seeing MSPs using ID Agent to keep their existing clients safe? I guess most MSP clients don't know their data is compromised until it's too late, right?

KL: That’s typical – something happens and they call in a panic that they have to go out there and spend X to try to resolve what had happened. The answer the question is,

‘absolutely’. We started in this channel roughly 18 months ago, and we had maybe two or three MSP partners. We're now well over 1,000 partners.

They're using the platform, and they're monetising the platform in a couple of different ways. Some are going to their organisations or customers and saying, ‘We just have to turn on monitoring, and it's X dollars a month.’ They're selling it as a monitoring service, or some are embedding that service within their security stack solution. It’s another facet of their bundled pricing models.

We’re seeing them go out two different ways - some are selling a standalone and some are bundling it in. One of the biggest benefits of this is that it’s’ eye-opening data.

Typically, what happens is the MSP goes out, sits down with the customer prospect, maybe they turn on the monitoring, but then they also started saying, ‘Well, this is why you need endpoint, this is why you need two factor, this is why you need backups, security awareness training, password manager,’ and on and on.

One of the things that we found is that the platform that we built is the catalyst to help the MSP sell all of the solutions that their customers should be buying. And it's changing the conversation from ‘security is an expense’, to the new mentality, and I think we're having a pretty significant impact on it.
This mentality is it's an ROI, it's not an expense anymore. You have to invest in these solutions up front, because the cost, particularly in Europe with things like GDPR, the cost in the backend is exponentially greater than the cost of frontend investing in security from the get-go.

RT: I used to be an MSP myself used to run MSP many, many years ago, I work with a lot of MSPs in the UK and Europe, and selling managed services can actually be a really difficult proposition.

As you've just said, there are all these different things are you need to do - a, b, and c. What I'm seeing a lot of MSPs do now, and I think the reason the buzz around ID Agent is so high is that it's giving real, measurable, practical reasons for clients:

‘Hey, look, your details are out there and have been compromised. And it's only a matter of time, not if but when it's only a matter of time, that something bad is going to happen here.’

Then the MSP can have the conversations about making sure that backups are in place, and all these other things. Would you agree that possibly some of the reason that the buzz around ID Agent is so high?

KL: I think so. And I think now MSPs are able to go in and say, ‘Look, this has to be a partnership. My job is to help keep you up and running and secure, but you have to do your job as well.’

One of the other ‘aha moments’ in some of these conversations is that the customer is making it harder for the MSP to protect them. You can go in and say, ‘You've got 20 or 30 or

100 or 200 employees' credentials out there and they have been compromised on LinkedIn and Dropbox or a dating site.'

There could be legitimate uses for business credentials on something like LinkedIn or Dropbox, but the other sites such as Facebook, there's no reason for that to occur. You shouldn't be using work credentials on a personal site.

It's giving the MSP the ability to say, 'This has to be a two-way street, because if I'm going to defend your perimeter, your uptime, backup and recovery, you've got to do your job as well. You're making it easier for somebody to go in and fake the credentials. They're using the keys to open the front door, the back door and the windows and exploit you.'

That's going to be harder for the MSP to ultimately detect, if the customer's not prepared to invest in the tools that would detect those exploits. I think it's the right market, right time. We tried to build this solution where it was very simplistic but really high impact.

That's really what it comes down to, why there's such a buzz and why we're having such a tremendous amount of growth and success in this market. We're really making that conversation that much easier for MSPs when they're in front of prospects and customers.

RT: I'll share with you that I actually had a conversation with a UK based MSP just last week who used ID Agent, and they had a conversation with one of their clients and said, 'Hey, you guys, you don't use Dropbox?' and the client said no. So, the MSP said, 'Well, we've actually got four accounts here using your business address, you do use Dropbox. Oh, and by the way, you've been compromised on it as well'.

That's another innovative use to uncover the fact that anybody can install a SaaS (Software as a Service) application getting up and running with an organisation as well.

KL: That's it. Some of the presentations that you've seen, or I give at speaking engagements is about how we're creating this culture of chaos. There are so many applications, and if you think about how many apps are on your phone, backed up on your corporate Wi Fi or network, or how many business SaaS applications that pop up every day that organisations are trialling or using, or not knowing they're using, it's accelerating.

Unfortunately, the paradigm of the email address and password way of authenticating and getting into the systems is not going to change anytime soon. There are some great bleeding-edge biometric-type authentication tools and platforms that are coming out, but even those have their challenges and risk.

It's human nature and the easiest thing for people to do in the path of least resistance and convenience for customers is a password. As we build all of these applications and tools for convenience, we're creating even more of a challenging environment for our MSPs and protecting their customers.

RT: We've talked about your explosive growth on your side of the Atlantic, and you're now making a lot of headway in the UK and Europe. We can't go very far in any podcast nowadays, without mentioning GDPR (General Data Protection Regulation). In terms of your

growth in Europe, how have you addressed the whole GDPR question? What does that look like for you as an organisation?

KL: The new four-letter word! We've taken GDPR very seriously. It's interesting, because some of our most progressive and early adopters were out of the UK, and that was fantastic. We had to hit pause, if you will, back last May when GDPR really came out and we started to understand the implications and impact of GDPR.

We wanted to make sure we understood fully what GDPR meant, not just to us, but to our partners and their customers. We've seen now that our platform is a tool to help address some of the compliance requirements of GDPR. It's not specifically defined, but in GDPR the regulators look more favourably if you are taking a more proactive approach to risk mitigation.

Part of that is understanding what your risk is out there on the dark web, what kind of credentials and what kind of data is out there. Our platform is having a pretty material impact on risk mitigation. If you're able to go in and show these credentials, and say, 'You need to step up your game and stop this behaviour and implement security awareness training.' It's having a 'check the box' impact on GDPR.
We took a pause between May and August to make sure we had everything fundamentally sound and we had all of our ducks in a row. That's why we're having such a big push into the European market, because the demand is there. We've had dozens and dozens of enquiries over the last several months, and we had to say, 'We're getting there and we'll get back to you soon.'

That Datto.com event that we were both at not too long ago was our first real push into the European market, and the response has been fantastic. People realise, and it's the same thing that we saw early on in the States and in Australia, is that this is the tool that's going to have that impact.

It's really going to help address some of the challenges with GDPR and getting your customers understand that they have to take GDPR seriously if they have any element of PII on their networks. That's been it's been a great tool and a catalyst in helping with that GDPR conversation that MSPS are having with their customers.

RT: I think for all the hullabaloo around GDPR, I would say it's actually been a good thing for MSPs across the board. You've been predominantly in North America and you mentioned Australia as well. Now you're in Europe, what have you found is the big differences that stand out to you between North American and European MSPs?

KL: I don't know if there's a substantial difference in our experience working with them. I think they approach solutions with a little bit more caution and diligence, which I think every organisation should. I think that's actually been a good thing.

We have very deep and substantive conversations with our European prospects and customers. They really want to understand what's behind the technology, and how it's really going to help.

I think that's been actually a great thing for us, because we've had a lot of early adopters and in the North American market and Australia, they've been progressive and quick to adopt, and I think we're going to see the same thing.

I think this is a newer solution and we have a different dynamic with the conglomeration of European countries and different philosophies across borders and stuff. I think that's led to having very engaged dialogue with our prospects and partners.

Maybe our sales process is lengthened a little bit, but quite candidly, I think it's a good thing because it gives us a chance to really educate our partners. They come into using our tool very much with a mindset of, 'How can I really use this to protect partners and how is it really going to benefit my organisation?'

Once they understand the tool and the impact, we do get that same level of excitement. I think that was one of the big things we noticed in Barcelona (in early November) that people want to really get a firm understanding of this solution before they jump in.

It might be just the stylistic difference between some of our partners over here and in the States versus Europe. I appreciate it, because it really gives us a chance to explain our mission and why we feel this is the right solution for everyone.

RT: Let me put my MSP hat on and ask one of the questions that I'm sure is on the tip of the tongue of people listening. From a technical perspective, do you offer any integration between ID Agent and a lot of the popular MSP tools out there, such as ConnectWise, Autotask PSA tools, these tools that MSPs live in most of the day. What does it look like from an integration perspective?

KL: As I mentioned, some of our early adopters were some of the more progressive folks over in the UK. One of the questions early on was, 'How can I use this under my single pane of glass concept?' To your point, thee partners live in either ConnectWise, AutoTask, Kaseya or a couple of the other big tools out there. That became an important initiative for us around May, when we were looking at GDPR.

We started down a path of integrating with ConnectWise and AutoTask first, because the most noise that we got were with those two platforms. Now, we are fully integrated.

If we get a hit, we find an email address and password for one of our MSP's customers and it will be fed right into their PSA. That way, they can monitor it within that tool, and they can create the workflows to be able to do password resets and bring security awareness to that individual that's had that compromise.

It has really helped to create that full automation, from us finding it, going into their management tools, and letting their customers known. That was a big request. On our springboard, I think we've got about 15 or so additional integrations that are in various parts of various cycles within the sprints we'll be announcing.

It's a large market and it's a very fragmented market, and it's interesting because there's Continuum camps, AutoTask camps, Kaseya camps, and we want to make sure that we

help enable our partners whatever camps they're in. We're going to build those integrations and make sure they have that automation and can run that single pane of glass concept.

It's a big initiative for us in this this fourth quarter, and certainly into 2019, around making it that much easier for partners to be able to adjust the data and then do something with it.

RT: Let's shift focus for just a minute from talking about managing clients and managing the dark web, to managing people. On a personal level I know you've been recognised twice on Smart CEOs Future 50 List and there are other accolades. You're now CEO of ID Agent - what skills would you say a good CEO needs?

KL: I think one of the things I've learned over the 17 years of running organisations, I thought early on that I was the smartest person in the room, but you have to lose that mentality and change your perspective.

I think I've kind of taken the stance of hire smarter people, and realise that smarter people in the room will bring their value to the business and help it grow. For me, it's been rule number one. This is coming from somebody that has a history degree, not a technical degree.

I try to take that philosophy when we're looking at building solutions, or day to day in the company, and maybe the benefit of having a history degree and being able to look back and trying to ponder what went right, what went wrong, Ultimately, you realise that the way you build a successful business is by bringing in people that are smarter.

We've got a tremendous CMO on our team, we've got a great Vice President of Development, Matt, who's out there on the road tirelessly. As an amazing advocate we just brought on a former MSP as well.

Dan Tomaszewski just joined us over the summer and he brings years and years of experience in MSP space. It's been invaluabl to get his insight to really understand how can we better help MSPs do their job and grow their business.

And as a result, our business will grow alongside of it. I subscribe to that philosophy, although maybe not early on, when I always thought I was the smartest one in the room.

I realised that you have to lose that pretty quick if you want to succeed in business and in life. My rule number one is, 'There are much, much smarter people out there, and if we can aggregate them and do good things, ultimately, it will help our customers and partners and everybody benefits.

RT: I love that philosophy and subscribe to it myself: surround yourself with people smarter than you and you'll go very far. What's next for ID Agent? What can we expect to see from you over the next few months? What are your goals for the company?

KL: Over the next several months, we'll actually be announcing some really interesting additions to not just the dark web platform but some platforms a little bit to the left and a little bit to the right of dark web ID. We are a security organisation, but when you break it down what our tool has fundamentally done is help our partners grow.

We've been balancing the fact that we're a security company with the fact that we're a company that's having tremendous impact on our MSPs and their revenue and growth. Some of the solutions that we'll be presenting here will be really designed to help further the MSPs ability to identify opportunities and grow.

There's going to be quite a bit of buzz on the frontend of the platform and helping MSPs identify and grow their business. And then downstream, there's going to be several more integrations that we announce and several more product enhancements.

We've been a tool that allows MSPs to sell all the other tools, we haven't taken this approach of, 'Well, we're a platform and now you have to buy our two factor and our security awareness training.' There are some schools of thought that say you should add that stuff in and be the platform.

But, as we talked about earlier, there are enough platforms out there. There are enough Continuums and AutoTasks and Dattos and so on We'll build in additional high value data and tools within the dark web platform that will further enable the MSP's ability to sell all the other stuff they've already invested in.

A vague way to answer your question, but we've got some really interesting, innovative solutions that we're going to be announcing here, and I think the MSP community is going to love it.

I'm really excited about it. 2018 has been an amazing year, no question, but I think we're even more bullish on 2019. A lot of 2019 is going to be spending a ton of time in Europe, helping our European partners. It's gonna be exciting.

RT: I'm excited to see where you go. As I said at the top of our call, I've rarely seen so much buzz for a company as I've seen for you. I've made a nuisance of myself trying to get you on the podcast for many months now, so I appreciate you taking the time out to speak with me today.

If anybody wants to reach out to you personally, Kevin, or to find out more about ID Agent, how can they get in touch with you?

KL: On our site: www.idagent.com, and we've got a number of ways to reach out and communicate with us. They can certainly send me a note: my email is klancaster@idagent.com. Feel free to reach out, as I try to get back to everybody as quickly as possible.

We've got all the social channels open and the website open, so anything we can do to help our partners succeed, because that's what we're all about. Don't hesitate to reach out.