David S.: Welcome to the Microsoft Industry Experiences Team Podcast. I'm your host, David Starr. In this series, you'll hear from leaders across various industries, discussing the impact of digital disruption and innovation, sharing how they've used Azure to transform their business. You can find our team online at aka.ms/indxp or on Twitter @industryXP.

All right listeners, welcome to the show today. We have a great episode ahead of us, looking at innovation in banking. I want to welcome Frances Zelazny, who works close with biotech CEO to conceptualize and formulate strategic initiatives. While on the marketing side she established comprehensive marketing strategy, including brand positioning, messaging, and execution.

Frances, welcome to the program.

Frances: Thanks for having me.

David S.: You bet. I wonder if you could first start out by telling us a little bit about your company, its mission, and customers.

Frances: Well, BioCatch is a digital identity company that is focusing on behavioral biometrics. We have a biometrics or technology use at look at the way people interact with online applications and devices in order to prevent identity theft and fraud.

The company is about five years old and today we monitor more than six billion transactions per month, mostly in the financial services arena, to prevent fake credit cards from being given out, to prevent account takeovers in online sessions, to otherwise provide a unique and streamlined customer experience in the digital channel.

David S.: How does that relate to the term behavioral biometric?

Frances: Behavioral biometrics used to be all about keyboard strokes and how fast you type, but actually today in the BioCatch world we're looking at two thousand different parameters of interactions. These can be categorized as physical behaviors, so the way you hold the phone, the way you type, how hard you press, whether you have a hand tremor, if you're right-handed, left-handed, so these are all physical behaviors; and then we look at cognitive behaviors. These are the choices that you make when you actually interact or fill out an online application.

For example, how you toggle between fields. One person might use a tab key, another person might use the enter key, somebody else might just put the cursor where they want it to go and the way we do these things distinguish us from one another but also from other things. Things like malware or robotic activity. We can also use techniques like what we call invisible challenges. These are subtle tests that we invoke inside a session that will further extract behavioral data, but a malware or bot won't be able to react to that challenge and if there's a robot access attack you'll see two different responses. So those are the unique ways that we use this technology in order to stop fraud in real time.

David S.: Are your customers able to see this fraud happening in real time?

Frances: The way the technology works is it's completely passive in the background, it doesn't change the user experience at all. As you conduct your online session if there's an anomaly or any kind of problem, the system will generate an alert, which then goes into the workflow or wheel engine of the bank. For example, they determine whether to stop the transaction, let it go if it's very low risk or a very low amount and it's not worth the escalation, or ask for a step up or a call to the call center or whatnot. Just yesterday actually, we heard from a customer that, using this methodology, we caught about a million dollars in an attempted international transfer attempt just yesterday.

David S.: Wow, congratulations. That's a fascinating story how you can tell all these different things by how someone interacts with software.

Frances: Yeah, the beautiful thing is we don't even think about it. It's almost like a reflex of how we do what we do and it's not something that you can steal or copy or lift up or even re-record because the invisible challenges are random and they're changeable so you don't really know that you're being "tested". And the other interesting thing is that what makes us unique from a behavioral perspective is different, so everybody's behavioral profile is based on different parameters so if you're a fraudster you don't know what the answer is and you don't know that you're being tested.

David S.: Against the typical behaviors of the owner of the account?

Frances: Mm-hmm (affirmative)

David S.: Where do you think banks suffer the most from fraud?

Frances: I think, a very general sense, the biggest challenge or where they suffer the most is the fact that fraud is not static and fraudsters are constantly changing their techniques and they're getting smarter and so it's like a game of whack-a-mole. You think you've got it solved and then the fraud or the problem appears somewhere else. Keeping up with this ever going on game of cat-and-mouse is just a losing proposition in the long run. They look at behavioral biometrics as a way to stem that.

And the other, I would say, broad challenge, is the continued hacks and breaches. Every time there is a data breach we typically focus on freezing the credit in order to stop an application, but the threat actually goes way beyond because fraudsters use information to build their data bases and increase their ability for social engineering and phishing and now there's vishing where people will call on the phone and convince the victim that they're a legitimate person and that they should transfer funds. And so the threat today is happening inside authenticated sessions and that's a big challenge.

David S.: Does behavioral biometrics cross all of those boundaries? You've got all these different ways people are trying to get into that fraud pipeline. Does behavioral biometrics essentially cover all of those?

Frances: Behavioral biometric can look at the end to end from a digital identity management perspective. So when we talk about digital onboarding using behavioral parameters to distinguish between legitimate users and people that are using stolen or synthetic identity inside an application. You can use behavioral biometrics in order to stop application fraud.

Consequently, inside an online session to prevent account takeover as the technology learns you it builds a profile and can apply there. And so it's unique in the sense that you can use it for both areas whereas most solutions or most approaches are either in the KYC identity proofing realm or in the authentication realm or in the fraud detection realm. Behavioral biometrics is broad enough that it covers all of them.

David S.: I was wondering if you could speak a little about your relationship with Microsoft and how its impacted your solution?

Frances: We've had a very good relationship with Microsoft from the very beginning. We actually were involved in the BizSpark program in our early days, and we've grown tremendously since then and we have, I would say, a very good technical relationship and very good business relationship as the BioCatch solution is built on by Azure platform and so we leverage a lot of the capabilities that Microsoft provides and we work very closely with the business team in order to capitalize on new opportunities.

David S.: How does your product fit into the stack of solutions that are out there?

Frances: Behavioral biometrics is quite complimentary in terms of working inside the enterprise with different solutions that are out there from a workflow perspective, and we have different partnerships that complement what we do. From a workflow perspective the identify proofing side, the role of applicant behavior is essentially to flag the fraudulent applications before you start going down the line with document authentication and other capabilities in order to get through the process faster and to minimize the disruption in the application flow. On the account takeovers piece, it's also generating a risk score that then guides the step up or some other workflows to manage the fraud and so this is not a rip and replace proposition, this is essentially a way to manage the actual fraud, reducing the fraud, but also reducing the friction that comes with escalations, disruption in the UI, and the other normal data collection or flow that you would want in the digital environment.

David S.: You must have to have a lightning-fast transaction speed.

Frances: It's real time essentially, and we're returning a risk score that's between zero and a thousand. The financial institution will decide what to do with the risk score when we return it. A thousand is most likely a fraud and zero is most likely the person and everywhere in between is where workflow and the rules come into play. So, in a retail environment if the transaction is five dollars, you may decide not to escalate because the cost of escalation is more than the actual potential risk whereas in a wealth management scenario, no matter what the potential risk is you want to flag it before it goes too far. It's very flexible in that sense.

David S.: Well Frances, thank you so much for being on this show. I learned a lot today, I appreciate it.

Frances: It was really my pleasure. Thank you so much for having me.

David S.: This is a new format for us on the Industry Experiences Podcast, this is one show and two interviews. Now let's get on with that second one.

Today we have Dekel Shavit, who is VP of Operations and Chief Information Security Officer at BioCatch and we have Uri Rivner, Chief Cyber Officer for BioCatch. We've already spoken with Frances and talked a bit about the product that BioCatch offers. Now we're going to talk a little bit more about how it works and what some of the technologies are.

So, gentlemen, we heard an overview of your product but could you describe for me behavioral biometrics as a study or as a topic?

Uri R: Yes, sure. Behavioral biometrics is the science of analyzing human interactions. People interact with the website or mobile app through their device so it would be the way you move the mouse, the way type information, the way you interact with a specific application, the way you move between fields, and the way you correct typos, and the way you scroll up and down. If you use a mobile device it's the way you hold it and touch it and scroll and swipe and essentially the way you interact. The thing is, we are creatures of habit and behavior biometrics is very good at continuously verifying and authenticating that it's indeed the regular user in the account. This is done by profiling the user. Using JavaScript to collect information or SDK if it's an iOS or Android device or any kind of mobile app. The data is then being used to generate a lot of features. We talk about thousands of various features. If you think about moving the mouse, then you have acceleration and you have up versus down and left versus right and the speeds and curves and all that, so it generates a lot of features.

And the same is around cognitive attributes. For example again, how do you move between fields and how do you correct mistakes and all that. The AI is used to then take all of this information and create a profile of the regular user behavior, and then it now looks at new activity. It will be able to spot an anomaly. For example, someone else operating inside the account or it could be some sort of tool. It could be remote access, which could be malware related, it could be a commercially available remote access tool, or it could be some sort of bot, or it could be some sort of social engineering attack with this script. The idea is to recognize the fact that as long the user behaves normally the system would recognize that, but if something happens and we do see an anomaly, then it's possible to alert about that and take the necessary actions. And this is done continuously.

We've had enough cases where the initial login, for example, was the real user logging in and the the session is being hijacked and an attacker is now inside the account and operating within the account making payments and all that. The behavior is going to be totally different. So the main use of behavior biometrics is to continuously verify the

user throughout the session, from the time you login until you finish the session, to recognize whether it's still you doing all of that, to identify threats, and to do all of that without any kind of friction, and even removing existing friction generated by the current security controls, or risk controls.

So typically if it's a bank and you come from a new device, like an untrusted device, or new location or you just do some strange activity the bank might challenge you or stop a transaction or delay the payment. Things like that. This is user escalation and today all of the digital services try to have a very smooth user experience. They want to remove those user escalations and there's a way to verify a user in a very frictionless manner seemingly by letting the user prove themselves and behave normally then this could eliminate a lot of these redundant security and risk controls, or at least minimize them. So this is the core capability of behavior biometrics, it's known as continuous authentication, but beyond that I would say that continuous authentication is kind of the mainstream use case for behavior biometrics. A lot of financial services are using that in Europe, in the U.S., in Latin America, in other parts of the world. We talk about dozens of millions of users that are being protected by behavior biometrics. This is for an existing user.

More recently, though, behavior biometrics also proved itself in several other scenarios that were initially quite impossible when you actually think about it to handle with this sort of technology. Starting with a new user, someone that is opening a new account, and of course if you open a new account online think about a credit card application. You go online and you want to provide your name and date of birth and social security and other identity data and essentially prove yourself and then get a credit card.

How would behavior biometric handle this sort of situation where a profile cannot be built? When we cannot establish a baseline of the regular user behavior? But behavior biometric is capable of stopping those extreme scenarios as well, because the criminals don't behave as normal people would. Here we talk about the number of analysis areas, I'm going to mention just a few. For example, if you open an account as a user you are not familiar with the process, but you're very familiar with the data. It's your own social security, as an example, or date of birth, or name. But if you're a criminal you're very familiar with the process of account opening because that's what you do in life, you know. You just attack those credit card companies and banks and other entities, but you're not familiar with the data and because of that the way you type information and insert data is going to be completely different. This would be one sort of scenario where advances in behavior biometrics now allow credit card companies or banks to defend against identity theft, synthetic IDs, and these sort of attacks.

Going to another extreme, what happens if it's the real person moving money, but this is because someone tricked him to do it? Or her to do it? In that scenario, behavior biometric is supposed to sense everything is fine because we do see the user, we do do see that it's the regular user patterns in terms of behavior, but the user is now under some sort of duress. The user is conducting a transaction without really realizing that they're not supposed to do that. It is coming from the regular device and location,

there's nothing wrong about the transaction, it's really done by the user. It's supposed to be quite impossible for behavior biometrics to detect that.

However, behavior biometric is now able to detect those sorts of extreme scenarios as well by looking at hundreds of very subtle features and indicators, or signals, and combine them together via AI. It would be around how distracted you are during the session, how hesitant you are around specific data elements, all sorts of very small changes in your behavior that are caused by the fact that you're now being guided by a criminal to move money from your account and it's a very stressful situation. So it's not just authentication capability or fraud detection capability in the sense of someone else operating inside your account, it could be you operating inside your account but you simply behave in a very abnormal way that correlates to these social engineering scams.

The bottom line, if you think about behavior biometrics, it's a set of very powerful signals that look at the way digital users behave online, or in mobile applications. They're extremely useful to both verify the user continuously with no friction, reduce existing friction, and handle things like identity theft, even social engineering attacks.

David S.: Sounds like you're building a fingerprint, an identifier if you will, of a user based on how they might use your application, how they might be accessing their data, and you use an AI to model behavior as identity. Is that about right?

Uri R: It's about right, although I would say that the idea is not to identify the person out of billions. The idea is to essentially build a baseline of the regular user behavior, and say that, whatever we see now, matches that behavior. Does it match the behavior or we see an anomaly in the behavior. And again, if we talk about these other scenarios, the idea is to recognize either criminal patterns in the behavior, or maybe signs of stress, distractions, other sort of behaviors, that would tell us something what the user is doing right now and their mindset, and all that.

In essence, you're right that we're building a profile of the user, not in order to identify them out of billions of people, but in order to know what is the regular baseline of the behavior in the account.

David S.: Thank you for the clarification. What role did Azure play for you guys in your solution? And what kind of solution are you running? Are you SAZ application, you got VMs up there, containers ... what are you guys doing with Azure?

Dekel: I'll take this one. First of all, it's worth mentioning that BioCatch was born to the cloud. We are actually a graduate of the BizSpark program. From day one, we're actually using Azure.

To specifically answer your question, we're using a mixture of SAZ and PAS. When we provide our solution to the customer, everything is running on top of Azure, and we use a mixture of services. We're fully containerized now, and there's actually an interesting story here, how Microsoft help us transform and evolve our solution because back in the days, in our old solution, when we just start up the company as part of the BizSpark

program. When you're a small start up, you don't design your solution for the first 50 million users, you design it for the first five million users. You don't think so scalable. That's the rule of the engagement. About 2 years ago, it seems that our solution was ... the business was going up, and our solution was expanding in capabilities. But it was becoming harder and harder to support it. We need to reinvent the solution because we spent too much time on maintenance and not enough time on innovation, and providing more value to our customer.

The solution back in the days was simply a bunch of VMs, collecting the data, analyzing it, and it was a lot of complexity in that.

What we did together with Microsoft, with a lot of investment from the technical people at Microsoft, was to completely re-engineer our technology stock. We are now fully open sourced. Everything is containerized and stateless, which actually means we can actually support any scale needed. It's much more cost effective, and it's easy to scale specific part of the system because we are stateless. This is all due to a lot of investment, as a partner, by Microsoft. We actually had people working with us on our solution. That was an amazing journey for me. We are now 100% containerized, mixture of SAZ and PAS, using a lot of services with AMD Azure platform. That's a lot of good investments that we got in. As a small company, having Microsoft in your back hand, basically helping with a lot of knowledge and technology, that's simply amazing.

David S.: Dekel, I know that one of things that really resonates with BioCatch is what we call digital stewardship for security and compliance. Could you talk a little bit about how you see the role that Microsoft plays in structuring your business and the technology behind it?

Dekel: Definitely. Again, it's an amazing partnership. We are catering to the most demanding organization on the face of the planet, and rightly so. The fact that we can leverage Microsoft to have good security posture, or actually what I call design to trust with our customer. With the help of Microsoft, it's nothing short of amazing.

Things like the Azure Trust Center, which makes my life so much easier, or the Azure Security Center, which I share with my customers to show them how we're handling security adds a great value. It simply removes obstacle from the table. When we're talking to customers, and they're asking the hard question around security, and I can bring up someone from Microsoft to help me teach the idea and logic that we have in place, that's a winning card. It makes everything much more seamless and easy, and again, it's a great partnership with a lot of value.

David S.: That's fantastic, Dekel. Really appreciate the confidence in Microsoft technology, and also the fact that you can rely on us to be there when you need us the most with your clients. What are excited about technology wise, either from an Azure standpoint, or from the financial services industry?

Dekel: You know, AI is probably the easy answer, but I think ... everybody's talking AI now, and it's more and more DataPlay coming. Data is the king that everybody understands, but

Data Insight is something that we see coming more and more in the FAS sector on how to leverage data to do more for your business.

David S.: Howard, you've been involved more in the relationship with BioCatch for awhile. Can you talk about that from Microsoft's perspective?

Howard: Sure, absolutely. And we really pride ourselves and work really hard to ensure that we have solutions to address our banking capital markets enterprise customers. Their industry needs and make it relevant to them. I always say, "teamwork makes the dream work." With BioCatch, they are a proven technology that will deliver a material ROI to banking clients.

One of the things that my relationship has been with several of the leaders within the organization over time with doing podcasts, interviews, videos, and in helping them with their go-to-markets. BioCatch is a recognized leader in the field of biometric authentication. It has proven its ability to reduce false positive alerts, reduce disruption for customer experience, and deliver a real cost savings. Coupled with Microsoft's cloud, BioCatch offers a scalable, reliable, and complete approach to businesses across the globe.

I would just say BioCatch is ready now. Things don't have to wait. This is not a wait and see situation. There's minimal level of effort required to integrate BioCatch into any financial institution that has existing fraud infrastructure. Additionally, by being native to Microsoft Cloud Azure, BioCatch is infinitely scalable, as Dekel mentioned before. I think it's been a fantastic partnership and continue to look forward to continued growth.

That's why I'd love to hear Dekel talk about his perspective. Dekel?

Dekel: Definitely. Would love to speak on that. I actually see Microsoft as a partner, an extension of our organization, both on the marketing side ... there are amazing examples of how Microsoft leverage their part to help us do more. There is no other organization on the face of this planet that understand enterprise like Microsoft. With our customer roster, that's simply a good match. They know how to talk to enterprise and leverage their capabilities to help us do more. That's on the go-to-market side.

On the technical side, same story here. It's dancing together. The fact that we can have a robust solid technology that works day in and day out, but it still at the same time innovate and push the technology further working with everybody at Microsoft asking the hard questions, getting hard answers, re-answers to day to day issues is simply amazing.

Again, it's an extension to the BioCatch organization. I really see this as an amazing thing we're doing together, and I'm hoping to leverage it more and more. This is for me a winning formula that I want to keep on doing.

David S.: Uri, thank you so much for being on this show. Dekel, thank you very much for being on this show as well, and Howard for joining us.

Thank you for joining us for this episode of the Microsoft Industry Experiences Team Podcast, the show that explores how industry experts are transforming businesses with Azure. Visit our team at aka.ms/indxp, and don't forget to join us for our next episode.