Honeywell: Deep Learning Improves Data Analysis

Transcript from August 7, 2019
Customer Spotlight Webinar

Tim Crawford: We have a stellar discussion set up to discuss one of the hottest topics facing enterprises today: transformation. Companies of all sizes are looking for ways to transform their organizations, products, and services to benefit their customers. Today, we will discuss how one company is transforming their security products to benefit customers in many ways.

In this webinar, we are joined by the team from Honeywell to discuss their transformation journey and how it benefited their customers. During our discussion, we will also examine Intel's role in working with the Honeywell team.

Today I'm joined by Tim Baker and Luis Rodriguez from Honeywell. Tim, Luis, welcome to the webinar.

Tim Baker: Thanks, Tim. Hello to everyone and thanks to Intel for allowing us to participate in this first spotlight webinar.

Luis Rodriguez: Yes, looking forward to this, this is going to be great.

Tim Crawford: Excellent, thanks guys. My name is Tim Crawford. I am a CIO strategic advisor at AVOA and I will be your host for today's discussion. Let's get right into it. Many people know about Honeywell as a $35 billion Fortune 100 company.

Tim, Luis, maybe you can take a minute and introduce about your group at Honeywell and what you are doing.

Tim Baker: Sure, I will start. This is Tim Baker and I lead the marketing and product management teams globally for Honeywell's Commercial Security Group. Commercial Security is part of Honeywell Building Technologies, a division within Honeywell, and the Honeywell Building Technologies division, as the name suggests, focuses specifically on serving businesses that own or occupy commercial property. Everything from small businesses to global enterprises to critical infrastructure.

Tim Crawford: Luis?

Luis Rodriguez: I am Luis Rodriguez. I am also on the Commercial Security Division, and my role is around the transformation that we are making into software industrial giants in IoT, so I help by building up the third-party ecosystem and also with our as-a-service strategy and recurring revenue strategy for the Commercial Security Division.

Tim Crawford: Perfect. Thanks, guys. So, let's set a baseline for our discussion and dive into who your customers are. Can you take a few minutes and help us understand what your division's customers look like, and the kinds of challenges that they typically have?

Tim Baker: Yes, so I guess I will start. As I mentioned, we operate globally and we serve a broad range of customers across the globe and their challenges vary. But there are some common themes for sure, across geographies and across user segments. As an example, customers generally are looking to detect threats before they occur. An example would be, an easy one that everyone can relate to are auto dealers. You take auto dealers as an example. Most are closed, or maybe all are closed on Sundays. And they typically want to protect the perimeter of their property, and know on a Sunday if somebody's loitering directly outside of their property, to prevent automobile vandalism, or someone coming into their property before that even occurs. That is a pretty common theme, certainly around perimeter protection but in other applications as well. Another one that I think is really common, most customers are putting a lot of manpower behind keeping their businesses secure. Especially in the enterprise space. But they are looking for ways to really drive efficiency and reduce the chances of human error. It is not about reducing cost but it's also about reducing the chances of someone making a mistake and potentially missing something critical. An example of that would be, on a large campus, guards can't necessarily be everywhere at all times. There is always an opportunity for them to miss something important. That is a challenge that they know they have and something that they would like to overcome.

Tim Crawford: Tim, when we were talking earlier, one of the things that came up that I think is pretty interesting is understanding the challenges that your customers have. Maybe you could share just a quick perspective on how you are learning more about your customers?

Tim Baker: Yes, as Honeywell Building Technologies, going into customers with that hat on, it is really about understanding their broader business challenges first. We spend a lot of time directly with customers at the end-user level, whether it is engaging them directly. For us, it is not just engaging with the security staff, but it is engaging with the IT staff, with the C-suite, with the operations folks, to understand specifically how security could potentially help them run their businesses better. And we do that not just through direct question and answering and meeting in conference rooms but also getting permission to go and observe freely how their operations work, because often times our customers won't necessarily articulate to us some of those challenges. It's the type of thing where you have to observe them directly and pull out those latent needs and business problems.

Luis Rodriguez: Yes, to add to that, what Tim Baker is saying about the customers maybe not understanding what they should ask for, there is a lot of this happening right now with the rate and pace of technology where there are so many new kinds of things coming out that customers don't always understand the art of the possible, but instead of starting with the technology and trying to find out what it can solve, if you start, as Tim was saying, with the customer problems and then working backwards in, it tends to be really productive.

Tim Crawford: That is great. I think that is an important aspect to bring out in our conversation, because quite often we don't talk about how we get these insights and how you are getting those insights is that firsthand knowledge.

Let's maybe double click a little bit into some of these pieces and talk about how the customers are using technology and the different ways that they are using technology.

Maybe you can take a minute and talk about how your customers are leveraging technology to solve some of these challenges.

Tim Baker: Sure. For us, one that is really exciting and really coming to fruition now is around video analytics. What video analytics has really brought to security is it has allowed us to take video as an unstructured data source and really start to synthesize meaningful insights from it. In layman's terms, it is about not having to rely on somebody staring at video to, from a human perspective, synthesize what you would glean from that. Perhaps viewing a fight and then reacting to it or something like that, it is allowing the analytics to do that work for you. From that perspective, we are able to then use this analytics to take that unstructured data, put it into a structured form that then we can use it in all sorts of ways, to help inform people, to feed into deep learning algorithms along with other sources of data, I think that we will get into that more a little bit later, how to use multiple sources of data and then really start to do some interesting things around solving problems for customers. One example that is fairly recent for us, that we've implemented across a handful of different customers is around detecting denylisted* individuals in public spaces, in K-12 schools. Using a combination of a database of known offenders, along with facial detection algorithms and marrying those two things and bringing them together. As you can imagine, having to have a single operator try to watch all video cameras in a large space and keep an eye out for those denylisted individuals is almost futile. It is really challenging. Now, what we've been able to do is leverage analytics to look at all those channels of video simultaneously, pick out those potential offenders and have that single operator focus on that area of concern, rather than having to try to watch all this white noise and sort out where there is potentially something bad happening.

Luis Rodriguez: One area where we are particularly focused in this is, as Tim Baker was saying, around schools. We started a schools initiative K-12 last year. It has evolved. We started off around technology, like we are talking about here, what are the different types of technology that schools can use, facial recognition, license plate recognition, loitering, to solve the use cases that they have, but it has evolved. We recently signed an alliance with a firm known as NCS4. They are based out of the University of Southern Mississippi. They get a lot of funding from the Department of Homeland Security. And think of when we bring technology, either ourselves or through partners, they bring the planning and testing part of it. They research best practices for keeping people, students safe. They research how to take technology and put it into a living lab and test it out and they will also train people who come in on with those best practices and on the technologies. For us, it gives us the best of both worlds. We bring technology, they bring expertise. We can test and improve our solutions and our technology there and this initiative is all about how do we then take that to schools, which is really about protecting who matters the most, and be able to deploy technology that some of these schools don't even know exists

and is viable, and that we can even help them, we have a grant writing program, in terms of affordability. The best thing of all this is, in addition to helping to protect what matters most using technology, if you take the use cases that are coming out of this, they can apply to basically anywhere where you have lots of people gathering, so that is going to help us to expand the safety net that we can create here.

Tim Crawford: And if I can bring it together a bit, Tim, when you talked about facial analytics, or video analytics, you have given some examples of facial recognition, but also behaviors, individual behaviors as well. I find that interesting because it is a complicated space, right?

Tim Baker: It is. Yes, that is going to take us a step further before we move on to the next topic. When you think about facial detection, the next thing behind running analytics directly on the video to detect faces, is to take it to behavioral recognition. We are starting to use behavioral recognition to do things like detecting fights breaking out in schools. I think that Luis's example around what we are doing with NCS4 is a perfect example. As you can imagine, a school administrator trying to keep an eye on everything that is happening around their school campus, again, it is a real challenge. If you have your video assistant potentially pushing a video clip of a fight breaking out outside of your school or in the cafeteria, it really allows them to address these issues before they really get out of hand. It is a great solution for schools that can also go to other applications, certainly public spaces, etc.

Tim Crawford: Sure, and one of the questions I am sure is bubbling up in people's minds right now is the whole regulatory compliance and privacy, which we are going to get to in a couple of slides here. So I want to hold that piece. As we talk about this technology, this is really complicated stuff, and requires a village to build it. There are important partners that come into that play, so I wanted to shift gears a little bit and talk about your partnership with Intel. Many people may think of Intel in different capacities, but Intel played a pretty significant role in working with you and partnering closely with you. Can you maybe take a few minutes and talk about your partnership and how Intel played a role in your technology, and more importantly, the innovation that you brought to customers?

Tim Baker: To be frank, we wouldn't be able to do what we are trying to do without some of the technology that Intel is bringing our way. Some specific examples of that are… For Honeywell, we cover a pretty broad range of applications and customer types, and especially when you look at our enterprise-scale customers, one of the values that we bring as Honeywell is being able to tailor and customize our solutions to our customers' needs. We can't really do that without having a pretty broad breadth of portfolio in terms of hardware solutions. I will be getting to specific examples around that but hardware solutions to be able to solve for these different applications and for us one really huge area of efficiency is to be able to have a single software solution that can be deployed or scaled across all of those different hardware platforms. That's again for us where Intel really provides value. The other part is OpenVINO™ [Toolkit] on Intel's partner ecosystem really adds some flexibility for us by simplifying how we partner with other analytic partners to develop more holistic solutions for our customers.

Luis Rodriguez: That partnership part of it is such an important part of the overall partnership. Intel is investing a lot in the partnership program, not just in things like the OpenVINO Toolkit or tools that make it simpler, but also in helping us, to introduce us to their partners, which can become our partners very easily, and that is going to help us to really be able to serve more customers' use cases more quickly, so that whole strength of that partnership program is also key to us.

Tim Baker: Connecting the dots between those various partners is really important for us because we just don't have all the answers, all the technology within Honeywell, even though Honeywell is a huge company, we have specific areas to focus, specific areas where we know we are good at and for us it's really important to partner with others. The whole purpose of having Luis and his team around driving ecosystems is around helping us bring together all these different partners into holistic solutions that seem unified for our customers in a single simplified experience. Going back to that scalability comment that I made, for us, we are doing everything from trying to leverage processors, at the [Intel] Atom® processor scale, potentially in cameras directly or near edge devices to do analytics and then, certainly in our network video recorders trying to take advantage of the various processors all the way to the [Intel®] Xeon® processors and in our enterprise-scale servers in the cloud and it's really important for us to not have to go redevelop software to work across those different platforms.

Tim Crawford: Beyond the breadth of portfolio, there was also some co-development that you worked on and I want to use this as the parlay between, showing the partnership but then also showing how it actually gained life in your particular situation, especially as we get to a very touchy subject around regulatory compliance and privacy. There was some co-development work that you did too, between Honeywell and Intel. I want to make sure that that comes into the conversation and you can share it with the audience. But maybe back up for a second and talk about some of the challenges. Honeywell is a global organization. This is a touchy area for us, for all of us today. How are you navigating through that complexity with your customers?

Tim Baker: From our standpoint, we are not, due to regulations, compliance, and privacy, when you look at the verticals that we focus on, like banking, critical infrastructure, and the pharmaceutical industry. We are used to having to deal with compliance regulations, but for us it's primarily been with things like fire and life safety systems or access control systems. To have this level of scrutiny now being brought to video is something that's been fairly new to us. It has kind of been a journey, but it's at least been one that we are familiar with following in other domains than Honeywell.

For us, where Intel has really helped us is to optimize our own solution specifically around GDPR. When I talk about compliance now applying to video that is specifically what I'm talking about, when I talk about privacy concerns. GDPR coming out of Europe was really what drove that revolution and has certainly extended beyond Europe now, it is being adopted in California and other places. For us, the important thing when you think about something like GDPR compliance is around how do you bring the compliance requirements around things like privacy masking video in real time to the same platforms that we are using today? Our customers, yes, they may have large servers on-premise or in the cloud, but at the client side they have to be able to do this privacy masking, potentially across multiple channels of video and so that's where Intel has really helped us, is to sort out how we do that client-side

GDPR privacy masking, down at the client level, on fairly lightweight hardware and allows us to do this really compute-intensive applications around privacy masking, without having to do that masking at the server side. And so what we do is, we actually use encrypted video to protect identities between video that is stored on the server, no matter where that server is, to the client, and then the client is able to decrypt and apply the masking appropriately. And that can be defeated as needed and where approved, as an example, if the authorities are wanting to look at video on a client to try to identify or understand where a potential perpetrator is.

Tim Crawford: Tim, can you maybe take a minute and explain what privacy masking is or how it would be seen to a customer or how they would experience that?

Tim Baker: Yes, quite simply, privacy masking is using video analytics to identify people within a scene and specifically masking, really the minimal amount possible, to protect their identity and privacy. The reason I say minimal amount possible is because you still want to be able to glean things from viewing that video without necessarily seeing the face behind whoever's doing the act. Again, that's where Intel's really been able to help us optimize, along with some of the partners on the OpenVINO platform, to mask just enough of that area with facial blurring or other techniques to be able to still make out the rest of what's happening in the video scene, and do that effectively and meeting those GDPR requirements.

Luis Rodriguez: Great. And the school example would be you are watching a video, everyone's face is masked but then the analytics figure out there's someone who is on the denylist and so their face automatically gets unfuzzed. It becomes visible so that somebody looking at that can confirm and take appropriate action. So that's usually how you would see it, a bunch of blurred faces. Some of the time, some of them can become visible.

Tim Crawford: Perfect. And I think that is great to understand because, again, it puts some reality to it so you can visualize what the customer would experience as they go through dealing with compliance and privacy in a real-world situation. So, as you go through these exercises and you've learned a lot along the path, I'm sure, what are some of those lessons that you picked up from your customers, from the experience, from the technology, from the innovation, that you could share with others?

Tim Baker: So, one of the big challenges, and this may seem fundamental, but whenever you are trying to convey a new solution like this, especially one that is as complicated, potentially, as bringing solutions around video analytics, deep learning, and AI to create a proactive security environment, it can get really easy to get caught up in the technology and, from our standpoint, trying to communicate this to customers initially was a challenge, because we are trying to do it in the context of these buzzwords. Ultimately what we realized we had to do was bring it back to the problems that we were actually solving and instead speak in terms of those problems that we were solving and then use the technology more as a means to explain the how. It really was around how do we get this message out in an effective way? I think that I've seen other companies also struggle with this, and I think that's actually slowed the adoption to some degree. Another thing that I would say has slowed the adoption is just how challenging it can be to deploy solutions that involve deep learning and AI, in particular for large

enterprise-scale customers. One of the challenges that you have is you are trying to get to a certain confidence level, preventing a higher false alarm rate or false positive rate, and there's an element of having to teach these algorithms and configure them on site, depending on the site that you are setting up. That can start to get pretty cost-prohibitive from a labor standpoint. What we've learned is that we have to figure out a way to preconfigure these algorithms, based on application, based on vertical or the site type. What we're starting to do, with the permission of our customers of course, is to leverage a lot of this massive install base that Honeywell has, and leverage a lot of the video and data that our customers are capturing to help pre-teach these algorithms so that, when they're deployed on site, they are not exactly turnkey, but they are maybe 80% preconfigured and we are able to set these systems up in a cost-effective way for our customers.

Luis Rodriguez: And then just to add to what Tim was saying that the overall notion of data governance is still very young in the industry. A lot of folks don't have, even though they are collecting a lot of data, the customers don't have a data governance policy or have signed anything about data governance. So being able to get that discussion and conversation going in their minds, to be able to get access to the right data, to be able to build models better, all that is something that needs to go faster, so that we can accelerate the rate and pace of the adoption of these new technologies.

Tim Crawford: This is great, this is just wonderful. Just as I think about where you have gone, what you have learned along the way, what's next? As you think about where you go from here and what's next, maybe just a quick thought from each of you in terms of where you go to.

Tim Baker: Yes, maybe an obvious one as the first next stop is just around how we automate deployment of deep learning solutions and computer vision solutions. Of course, we will do what I mentioned around the pre-teaching these algorithms. But what are the other tools that we can provide to our integrators, our installers, our end users, to help deploy these systems across a broader audience and make this mainstream because we think there is so much value for our customers if we are able to do that. One of the other things that I think is a really interesting space and emerging now on the buildings realm, is around bringing computer vision capability to mainstream access control. And you see it all the time, certainly it is table stakes for mobile phones and tablets to use facial recognition as an example to log into your computer, to your phone. But there are unique challenges that come with trying to do that and deploy that in a building environment. I've seen a lot of companies dipping their toes into trying to do that, trying to do video-based access control, but I think that our opportunity as Honeywell is, just like we did with GDPR, partner with Intel here and really make a big leap forward. That is an area that we're certainly looking to explore further.

Luis Rodriguez: I would just add quickly that it is also about being able to take different types of data sources beyond video. There is audio, there is stuff that people write online, even the weather can come into play in some of these cases, but being able to do take a AI-cognitive type of view of how to better predict, so we can prevent in a more effective way. There is a lot of work going on in that, just keeping on top of that and using our customers' feedback to help try that as well.

Tim Baker: For us, it's all about making security systems proactive instead of reactive and really for the building occupants, systems that are falling into the background and really only coming alive when there's a threat or a concern.

Tim Crawford: That is great. Tim, Luis, thank you both for helping us all understand the work that you are doing and how it has transformed both your solutions, as well as helping customers transform how they work and ultimately the value they are bringing to their stakeholders.

As we move to the next section of the webinar, the Q&A section. The first question: You mentioned OpenVINO. What is it and how exactly is it helping with these solutions?

Tim Baker: I am going to let Luis comment first and then I'll add my two cents to this one.

Luis Rodriguez: It is a toolkit that allows you to improve how quickly you can build on top of the Intel machine learning frameworks for computer vision. And so it helps in two different ways. One, it gives you a lot of prepackaged code and tools that you can use to get up-to-speed more quickly, but it also adds consistency, so that folks who build on top, build in a consistent way which makes it easier for folks like Honeywell to deploy in a consistent way. The more bespokeness you introduce into that whole process, the harder it is to maintain and support the system, so it really adds a very powerful element of consistency for us.

Tim Crawford: I have another question from the audience. When you think about video surveillance solutions and scale, specifically, and observing change. We talked about the auto dealership example, we talked about the school. How do you watch the perimeter, as opposed to just a specific aspect of that particular area? So maybe it's a question of scale, how you get more specific into particular areas or even broader areas that might include maybe a whole city or a much larger coverage area?

Tim Baker: Yes, it's a good question. I would say that the customer type or vertical that's really at the forefront here is and has been in the space for a while, are the gaming industry, casinos. Of course, casinos are huge expensive spaces and you see video being used extensively in casinos. And, essentially, if you go into an operations room in a casino what you see is a handful of operators staring at a large bank of monitors, and they are very specially trained. It takes a long time to really build up the capability to be able to do that.

Again, you are relying on this human element to synthesize all this data that they are trying to take in, this unstructured data, and sort out where you've potentially got an issue. Where the solutions that we talked about today come in and leveraging video surveillance allows you to really be able to do that much more effectively, and because of that you can leverage video surveillance to grow the scale on which you want to do this. Whereas before, if you lost your child in a theme park you'd have to notify security and security would have to just keep an eye out and look for a crying child, hoping to find them by chance. Whereas with video surveillance solutions, and some of the solutions we talked about, we talked about looking for denylisted folks, but you can also take a mobile phone shot of that child or

have it shared from the parents off of their phone, feed that into the video surveillance system, do a smart search across all your channels of video and find the child much more quickly. That is an example of where you can use something like this in a way that maybe is different than how you did it in the past.

Luis Rodriguez: I was just going to add one other thing to the user experience perspective. You can actually—there's technology today where you can automatically piece together different video feeds. Even video feeds from third parties, like Tim was saying. So you for putting together this mosaic that then can be further analyzed and so you can find where somebody walked to, from one place to the other, or if you're looking for a particular type of behavior, you can spot that forensically as well. This field is becoming much...This is one where there is a lot of new innovation coming out of.

Tim Crawford: That is great.

When you think about the breadth of customers that you are seeing, are there particular industries that are leading the charge when it comes to innovation, or driving you to think differently about solving some of these problems?

Tim Baker: Is the question around customer types that are driving that innovation or partners that are driving that innovation?

Tim Crawford: The customer types. Are there particular industries or customer types that are leading the charge?

Tim Baker: I would say that for us, it really depends on the charge, their specific application. As an example, in the pharmaceutical industry there is constant change happening, and one interesting space in the US right now is around marijuana growing and dispensaries.

That brings a whole different set of challenges around regulating the people. Essentially those growing facilities are treated as true pharmaceutical facilities. You are having to take something that is somewhat agricultural nature and now having to apply pharmaceutical grade compliance and regulation to it. That is certainly pushing the envelope in terms of how we deploy this technology.

I mentioned the gaming industry is a big one. The big challenge of the gaming industry is really trying to do the type of work that we are doing, on a really large scale. The typical casino has between 2,000 and 4,000 channels of video. So it is just a tremendous amount of data coming in. Again, how do you manage all that data and find what you are looking for?

Those are a couple that are really pushing it for us. On the perimeter protection side, certainly critical infrastructure. There is a lot of concerns these days around terrorist threats. I can tell you that around my house that the power delivery stations and substations all of a sudden I'm seeing all sorts of security go up around those. We are engaging them on new innovative ways to manage perimeter protection. At the expanses of those large facilities. Those are just a few examples.

Tim Crawford: That is great. Our next question. I find this question actually really interesting. Is it possible to get the solution granular enough so that you could quickly identify an approaching threat but at the same time be able to direct resources to people that need help the most?

It's almost bringing some intelligence to it beyond just identifying the threat, but also maybe helping provide some direction. What are your thoughts there?

Luis Rodriguez: From schools' perspective, that's definitely been something that is being discussed a lot more these days. There is technology today to do a lot more than what you see as the more traditional, like just lock the school down and call the police. You have systems now that can automatically call the police, that can provide, if there are weapons detected or a shot detected, can provide situational awareness with the video, but at the same time, if you know where the threats are, and you know where were the people are, then you can start trying to figure out, okay, now that you know that, where do you direct the ambulances to? Where do you direct other resources to help people? And it's because of being able to identify these threats very quickly and with speed, that you can then start trying to buy time to keep those threats away while you provide help to the people that need to get to safety or someone gets hurt, who is hurt, and how to get help to them more quickly through integrated communications.

So mass communications, integrated communications, that is another piece of it that, when you get that part in there, really takes the response to the next level.

Tim Baker: Just to further that, we have got an integrated security software suite called Pro-Watch. One of the really nice things about Pro-Watch is you can take multiple sources of data and essentially program in logic in terms of how you want to respond to that data. With something like object recognition analytics, you could detect if somebody had a gun or a knife in their hand, and that is going to invoke a different response than perhaps two people fighting. That potentially escalates the type of response. Pro-Watch can tailor the response based on the type of alarm that's coming in, and then also deploy a set of actions or standard operating procedure, again, based on the type of threat that's happening or occurring. Certainly that's the line of thinking built into our solutions.

Tim Crawford: Great. I have another question asking about the solutions themselves that you're doing for customers, how customized or bespoke are client-level commercial security solutions? Do they entail working with partners like Intel on a project-by-project basis to get the technology in place or is it more standardized?

Tim Baker: That is a really good question. I would say that it really varies on the user segment. In the small- to medium-business space, typically our solutions are fairly turnkey and it is a similar experience to what you might get if you are deploying even in residential security solutions, where you have the software itself walking you through as an end user, potentially, or a less knowledgeable installer or integrator doing that set up, and the system more or less preconfigured or configuring on the fly based on simple questions.

When you get to enterprise-scale applications, they are absolutely customized and specific to the site, to the needs of the business. There are certainly commonalities when you talk about across verticals, so we have pre-canned, preconfigured systems that we would deploy in the pharmaceutical industry, versus the banking industry etc., that has those built-in standard operating procedures for those industries etc. Generally speaking, there is a fair amount of customization.

As far as working with partners like Intel, I would say that happens on a fairly regular basis. What will happen is we get a new request, or the challenge to solve a new type of problem with an enterprise scale customer, we will partner with somebody like Intel to go solve that problem. And very oftentimes will then add that to our portfolio and use it across other customers in the future. I would say those types of scenarios come up on a fairly regular basis.

Tim Crawford: I want to thank Tim and Luis from Honeywell along with the team at Intel and the audience for attending this webinar.