Season 3 | Episode 44

New Security Threats in our Work-From-Home Era

Gene Marks

CPA, Columnist, and Host

Daniel Clayton

VP of Global Security Services
and Support at Bitdefender

Announcer:
Welcome to Thrive a Paychex business podcast where you'll hear timely insights to help you navigate marketplace dynamics and propel your business forward. Here's your host, Gene Marks.

Gene Marks:
All right everybody, this is Gene Marks. I'm here with Daniel Clayton. Daniel is the VP of global security services and support at Bitdefender. Daniel, first of all, thank you so much for joining me.

Daniel Clayton:
I'm really pleased to be here. Thank you for the invitation.

Gene Marks:
Sure. So first of all, let's talk about you and Bitdefender and then I got a bunch of questions for you, but let's start with Bitdefender first. Tell us a little bit about the company and what you do for the company.

Daniel Clayton:
Yeah, I'd love to. So Bitdefender, surprisingly, really for a cybersecurity company we've been around for about 20 years originally founded by Florin Talpes, our CEO and founder, largely because he felt that there wasn't enough innovation being brought to the cyberspace about 20 years ago. He felt the bad guys were really innovative, were doing a lot of cool things and really were beating and outpacing defenders. So he built the company to be a kind of voice of innovation, I guess, within, within the cybersecurity world. And that's really reflected in the way that we do business today. We're a 1700-person business, about 800 of that number are engineers. And about 400 of those are dedicated to research and development. So, right, that's a massive statement about how important research and development is to us. And we really ... you know, you see that in a lot of the things that we've embedded into our technology. A great example would be that we've been using artificial intelligence for about 12 years now, way ahead of anybody else.

Daniel Clayton:
It was ... It's kind of a standard fare for us now. We've been working with it for a long time. Also worth noting: I think we've got about 285 threat researchers on staff as well, who do nothing but, you know, stay in touch with the threat landscape, analyze what bad guys are doing, and really have an eye on the threat landscape

and how it's evolving, so that we can deal with it. And that sort of brings me to where I fit in. You know, the company has prided itself on bringing innovation to the way that customers are able to defend themselves. And in today's threat landscape, one of the things that we are seeing is that, it's very difficult for a lot of organizations to defend themselves effectively without high levels of expertise and resources.

Daniel Clayton:
You know, the types of 24/7 eyes-on-glass operation stuff that is just really expensive from, really difficult to build and maintain. So Bitdefender wanted to turn that round for our customers. So they approached me and asked if I would come to Bitdefender to build a services arm. So, you know, I was happy to go, happy to be involved with a company with such a pedigree. And we've built a security operations center and now a managed detect-and-response service, which really enables us to keep on innovating for our customers.

Gene Marks:
You know I — and I do want to get into some of the threats that we're facing — but as you know, and I think I told you before we even started this conversation, like, our audience are small business owners. So as a small business owner, a lot of us have already moved our stuff to the cloud. So we've got our stuff managed by some managed service provider, or we're using a cloud-based application. In addition to that, if we're running Windows, we're running iOS on our devices, they come with built-in security, you know right? I mean, that's what Windows has, Microsoft has their own thing. So where does Bitdefender fit into all of that? If I'm a business owner, what am I buying from you?

Daniel Clayton:
Yeah, sure. So we started off really providing that service, right? We were an AV company initially, an anti-malware company. And then as endpoint protection over the years has evolved from EPP, endpoint protection, to EDR, and now MDR, what you are really getting from us now is, in addition to that blocking capability on the endpoint, the ability to identify the types of malware that bad guys are using to target businesses and individuals as well. But also we use our AI to start to predict how might this malware evolve and change? And we're able to block that as well. And now what we've added to that is we're able to surface a lot of information from the endpoint and put that in front of security analysts or security engineers, the people within the company who know the network, that know what the telemetry should look like, and then they can look at the information that we give them and identify if anything in the network is anomalous at the moment.

Daniel Clayton:
And anomaly detection is really where everything's going at the moment, right? You, we have to be able to understand what an environment should look like, and if we can do that, then we can start hunting down things which are anomalous. And so Bitdefender really is providing that full suite of everything that comes from the endpoint. And then of course, it just about a bit just about to drop as well. I don't know if your listeners are well versed in the idea of XDR, but XDR is this concept of adding more data streams to the analytics so that we can not just see what's going on on the endpoint, but see what's happening within our email, what's happening within network, cloud infrastructure, bringing everything together so that analysts can have a full picture of what's going on in the environment.

Gene Marks:
Got it. And so your applications though, they are running — when you say endpoints —they're running on our local devices. So they are looking at whatever interactions are going on between the users and the outside world, and hopefully catching it, or at least alerting before it gets into one of our managed systems wherever they happen to be. Is that a fair assumption?

Daniel Clayton:
Absolutely.

Gene Marks:
Okay. As we're talking about this right now, a big conflict going on between in Russia and Ukraine, there is a, you know, there is concern that, in defending itself or maybe as part of an attack Russia may institute some attacks on cyberattacks on the U.S. Should we be worried about that, Daniel? And is there anything I should be thinking about that it could be impacting my business?

Daniel Clayton:
Yeah. I think there's lots of levels to be worried about, right? I think, first of all, this is the first time we've really seen hybrid warfare get powered out, right? That combination of boots on the ground and then cyber disruption as well. So I think everybody at a strategic level is looking to see how that plays out. I'm sure the Chinese are paying a lot of attention to how successful that is. So I think as you know, lovers of democracy and living in a democratic country, there's reason for us to be paying attention to that. The next level I would say is that Russia is really good at this stuff, right? Russia is really good at misinformation and disinformation. And then using disruption that maybe going on in one area to go and achieve its goals in a slightly different area, not often with Russia, you need to look in the other direction, right? Not the area that they're pointing us to.

Daniel Clayton:
And again, these are things that at a national level and become is, are probably paying a lot of attention to at the moment. I think in terms of the rest of us, what we need to be focused on at the moment is that there's a lot of cyber criminals out there. There's a lot of bad stuff that is going on, and they're very opportunistic. And so what we are seeing now is a lot of bad guys who are really sort of jumping on the bandwagon and using the emotions and everything that's about everything that's happening in the Ukraine and just seeing it all as an opportunity. So we are seeing a lot of phishing, a lot of getting people to click on things because they want to donate to the effort in the Ukraine, or they want to help Ukrainian people. There's a lot of opportunity there to get people to go and click on things. And there's also a lot of opportunities to get people, to download things that they shouldn't. You know, just click on this thing, download this link, download this link, and we'll send you some information you know, "to help you understand what's going on in Ukraine."

Daniel Clayton:
So there's a lot of this kind of opportunistic phishing attacks that's going on at the moment. And what that does is it opens up people to things like ransomware attacks as well. So if you click on something that you shouldn't, it's very easy then for a cybercriminal to steal your credentials, and if they steal your credentials, they can access your network. And that really brings in a whole gamut of, of badness that we need to be able to deal with — you know, ransomware probably being the most common one.

Daniel Clayton:
So I think that would be my biggest piece of advice to the listeners, to the podcast at the moment, is that be very, very wary about all of this stuff, that's out there, all of these emails that you are getting, or Facebook links, or whatever that purport to be about the Ukraine or are offering to give you the opportunity to help in the Ukraine. And just make sure you are confident in the sources that they go back to, and that it's actually a legitimate piece of information.

Gene Marks:

It's great advice. You really do make me think. If you're opportunistic enough and you're a hacker, you really can't jump on whatever the news story is at the moment, right, and go out there, phishing for people to click on, to donate to ... You know what, I wrote about just like a week or so ago, Daniel, is that you've heard about, I'm sure that there's this new regulation that a lot of the payment services now, Venmo and PayPal and Zelle, they're going to have to report transactions that they have from freelancers and independent contractors. A lot of people that would listen to this podcast, they're going to be getting these new, their 1099 reports at the end of the year, because they're now these payment services are required to report this information to the IRS.

Gene Marks:
And all of those services have already said, "We don't have complete information, so we're going to have to be going out and asking our customers for this information." And to me, that's like a recipe for a big problem. I think that in the second half of 2022, a lot of business owners, a lot of freelancers, a lot of independent contractors, a lot of people that use these payment services, they'll be getting a legitimate request from these payment services saying, "Hey we need to verify this information, or can you submit this information so we can file these reports?" But I also get the feeling that there's going to be a lot of opportunistic people out there, like you just mentioned, also looking for that confidential information. I'm assuming that this kind of stuff happens when the opportunities arise. Is that a fair statement?

Daniel Clayton:
Yeah, absolutely. And there's really no ... There's no limit to what they will take advantage of. We saw in the elections back in the last elections, back in 2020. We saw the same thing in 2016, people getting very emotive about certain things and then bad guys using that to socially engineer and phish people. We saw the same thing with the pandemic. Now you would think something like a global pandemic would be–

Gene Marks:
Bring out the best in people.

Daniel Clayton:
You know, would be off-limit. But not a bit of it. We saw it, I think one of the ... In fact, I think it was the largest attack vector throughout COVID has been phishing using pandemic-related materials. So yeah, absolutely. And this will be another opportunity. I don't have any doubt at all that it will be one that is used to target people who are going to be who will have obligations with these regulations.

Gene Marks:
Okay. So phishing really, I mean, our best defense is to be smarter. Maybe if you're an employer, you'll get some training for your employees. You need to make sure that you can recognize these phishing emails before you just automatically click on a link. Because again, if you click on something and it'll either take you to a website that can download malware, or it might cause you to download a document or download the malware directly that can get into your system, whether it's cloud-based or not. So if you're listening to this, you know, these phishing attacks, these are going to continue on. You have to be very, very careful. You mentioned about the increase in ransomware, a lot of that is being driven by working from home. So as employers are now going back to the — you know back, opening up their offices. Everywhere I'm reading people basically don't want to go back to the office. They want to keep working from home.

Gene Marks:
A lot of employers are ... They're scrambling to come up with hybrid policies. Bottom line is we're going to have a lot more working from home, and working remote people than ever before. The workplace has

changed, and that's just a fact. So when we're at home, our environments are not so great when it comes to security. What advice do you have for our listeners to make sure to, at least — you can't guarantee it — but to minimize the potential threats, security threats that their work-from-home employees could be facing, which could ultimately lead back to their own company systems. Give us some of your thoughts.

Daniel Clayton:
Yeah. So there's so many things, like lots of levels to think of this. I think that I agree with the original statement that you made, right. This remote working is here to stay, right? And there's no doubt that some offices are opening back up again, and there's going to be some sort of hybrid approach. Now, in some ways that's worse, right? In some ways, now you are dealing with both situations, right? Where you got some people behind the firewalls at the office, but then you've got on two or three days of the week, and then they're at home on the other days. There's all sorts of threats that are involved with that, all sorts of things that we need to worry about. I think one of the biggest ones is it's very easy when people are at home to get distracted, to get tired. It's maybe counterintuitive, but a lot of research out there points to the fact that people actually work longer hours and work harder when they're working from home, and a distracted employee is much more likely to click on something that they shouldn't click on.

Daniel Clayton:
And so that makes awareness, training and phishing awareness training really, really important. Like really help people to understand the risk of phishing, what it looks like, how they can be phished. And it's not just emails anymore. We're seeing increasing examples now of phishing taking place over the phone or through SMS text messages, and these types of things. So we've got to be on our guard–

Gene Marks:
It's called smishing with SMS, right?

Daniel Clayton:
Yeah. That's right. So these are things that we got to be really careful about and make sure our workforce is aware of them. I think wherever possible, we need to try to make sure our workforce are using managed devices. You know, it's much easier when you're at home. You've maybe given them a laptop, a really good laptop that they can work from. But if they've got a really nice, comfortable office at home with a big desktop in there, and all their speakers and webcam and everything tied up to it, they, there's a possibility that they might start working from their own computer and not from the managed device that you've given them. That then takes them outside of all the protections that you've put in place, right? So having all the correct controls in place to manage people's devices at home, manage their remote devices, wherever possible as well.

Daniel Clayton:
We see a lot more now, people working from their phones in the evening, sat in front of the couch as well. So these are things that we've got to be really careful of. So, I think that's the first thing. And a lot of that is really about awareness. The next thing for me really is that we have to accept that we are never going to be a 100% perfect. You know, the reality is that even the organizations, even big organizations that carry out phishing training exercises, 90% is a really good score, right? If only 10% of those phishing emails actually get clicked on across the company, that's a really big score. But it's bad enough that it can take the company down because it only takes one click from one employee on the wrong email, and it can be devastating, especially to a small business, right?

Daniel Clayton:
So making sure that we've got something in place to deal with that type of event when it happens, right? And ideally, the right way to do this now is to have some sort of monitoring capability in place. And that requires a couple of things. First of all, it means that you have to have visibility over your network. You need to know what your network looks like, and you need to have something on the network that can surface information to your team, to your security team, so that they can look at what it should look like in order to then identify something which is anomalous, right? So awareness training, and then some sort of monitoring and ideally detect and response capabilities.

Daniel Clayton:
So if we see something that we know is bad, do we have something in place to identify it and then deal with it? And these are hard things to do, especially from the small businesses, but there's a lot of services out there. Now you can outsource this stuff. Now we really are in a position today where even small businesses can outsource the type of capability that five years ago was really reserved for Fortune 500 companies, right? You can get eyes-on-glass now, you can get visibility into your network and a response capability for prices of which are certainly worth investing in.

Gene Marks:
And again, if you're listening to this right now what Daniel's saying is a 100% right, and there a plenty of resources that are out there to help you. And by the way, I can recommend some resources, if you want. I know lots of IT firms all around the country that provide these services. They cost — I mean, this is now an added cost that a business has to incur to operate in 2022, because this is the environment that we're in. And that is just the fact. The other cost also, that I think, Daniel, if you can comment on, is communication with your employees.

Gene Marks:
I mean, some ... You're giving the employees the benefit to work at home, which is fine. But there is a trade-off there you're going to ask for something in return. You're saying, "Okay, well, listen, you've got the flexibility. You're working from home. You've got your slippers on. That's all great. However, we need to monitor what you're doing. Not that we need to track your clicks and everywhere you are, whatever, but our, IT firm needs to make sure that you're not downloading anything wrong. That you're okay." Someone also tells me that, some IT experts say, that the hardware within our homes are also a risk. And I'm wondering if maybe you've got some thoughts on that as well. Routers ... my Amazon device behind me — which I'm not even going to say the name, because she'll get involved in this conversation. You know, tell us about the risks of those, of the hardware that's in a home, for those work-from-home workers.

Daniel Clayton:
Yeah, absolutely. I mean, you are ... any security program is only as strong as its weakest link. And the moment that we take people out from behind the firewalls and the controls and the policies and procedures that we have in place within the office — where you're probably being watched by a security team of some sort, whether it's one or two people or 50 people, it doesn't matter — someone is paying attention to it. And then you take them home, and all of a sudden you are at the mercy of however that family has its IT equipment set up. And the reality today is that a lot of the, a lot of the hardware that we using today, we've learned over the last couple of years that the supply chain plays a massive part and the supply chain is vastly complex.

Daniel Clayton:
And so a lot of these component parts are coming from China and Korea and you know, Asia and different places. And so we don't know what's on the chip, right? We don't know of the potential for something bad

to be embedded within the hardware. And we've certainly seen it with things like USB devices, that things that you can buy on Amazon, and you can buy online, that they come from, they come from China or other countries. And when you plug them into your computer, there's already a folder with software in there. It's already code on there. And so these things can be doing all sorts of bad things. IoT devices that may be in your environment. And also you may have hardware in your home network that is, which is from a perfectly safe source, that there is no major issue with, but it's been compromised.

Daniel Clayton:
You know, you might have a 10-year-old son who plays a lot of Fortnite, or a lot of Roblox or something, has clicked on something that shouldn't, and your home network is already compromised. So it's absolutely — and I agree with you entirely — it's absolutely within the reasonable remit of a company to require that when the company's data is at risk, that there is some sort of element of control over that data. Whether that's — and there's lots of ways to do that, right? You can provide the devices that you expect your employee to access data from. You can … Whether that's a laptop or BYOD or phones, you can give them the opportunity to use their own device, but you put some sort of management software on there, so that you can see what's going on and you can put controls in place to stop things being downloaded or move to personal folders or anything else.

Daniel Clayton:
So there are ways around this, which are very important. And I think for small businesses, it's really important to focus on the basics a lot of the time, right? Make sure multifactor is being applied, right? Multifactor is so much more important than a lot of things I see small businesses spending money on. It's really easy in the security industry. We get focused on the latest flex capacitor, right? The latest shining tool that we've seen or heard about on the radio, seen on the TV or heard about on the radio, right? And a lot of those tools may be really valuable to you, but if you are a small business with a small budget, you've really got to make sure that you spend your money in the right places and get as big as bang for the buck as you can in terms of protecting the company. And so I would urge you to put multifactor in place long before you start looking at a vendor selection process for an IDS or something like that.

Gene Marks:
All right. We only have a few minutes left, but I did want to cover one final topic and that's near and dear to my heart, which is travel. So I travel a lot. I have a separate laptop. Let me tell you what I do, and let me get your feedback, what I'm doing right or wrong. I have a VPN software on my laptop. I use Tunnel Bear is the name of the product. So whenever I have to connect to a public Wi-Fi, like my hotel router, or you know, in an airport, I do it through my VPN. So it's encrypted going back and forth. And it's very inexpensive.

Gene Marks:
Having said that, I try really hard not to do that. [Chuckles.] So if I'm in an airport, I'm trying to use my … I have, like, a Verizon phone. So I try to do from my own hotspot, because that seems to be the most secure thing to do. Tell me, if that makes sense to you, and also tell me if you have any other thoughts for our listeners that do a lot of business travel, to make sure they keep themselves safe and secure while they're on the road.

Daniel Clayton:
Yeah. The processes that you have in place make a lot of sense. We do similar things. We have different laptops that we will allow employees to take to different countries, depending on the level of risk that we associate with that country. Their level of access will be restricted based on where they're going, right?

Gene Marks:
Wow.

Daniel Clayton:
And so it makes a lot of sense that you are taking that type of precaution. I think in an [crosstalk]

Gene Marks:
And if I can interrupt you to say I have that rule for like, just in the U.S., based on the states that I go to. Like I have, it's always a much higher risk if you go to Florida, because it's Florida, you know what I mean? Whereas if I'm in some other place. I'm just kidding by the way. It is–

Daniel Clayton:
[inaudible]

Gene Marks:
It's just a riskier state in general.

Daniel Clayton:
Yeah. There–

Gene Marks:
Carry on.

Daniel Clayton:
Sorry.

Gene Marks:
No, go ahead. I'm sorry.

Daniel Clayton:
So it makes a lot of sense, right? I think that if I was to give ... Can I give a company advice about the way to approach the problem, right? The first thing is that you also have to treat it like gambling, right? You don't gamble with things that you're not prepared to lose, is the first thing. And the second thing that I would say is that, you need to assume that it's going to be compromised, right? Assume that it's going to be compromised. And then ask yourself the question, what happens next, right? So if you do that, it's going to drive you to put in place things like encryption, right? If my data gets stolen, if I know that I'm going to get compromised because I'm logging onto a network at the airport, and someone's going to see my data, it needs to be encrypted, right?

Daniel Clayton:
And so let's make sure that everything on this laptop is encrypted, that people can't see it. Let's make sure that if we're going to access another network, we've got multifactor authentication in place. There's something that we can use as a fail-safe to make sure that, just being in the airport and being on an insecure network, isn't going to be enough. So you know, I think with all things security, travel is a risk management proposition, you know? At the end of the day, it's a business. We have to travel in order to achieve the business objectives that we want to achieve.

Daniel Clayton:
And the question for the security team is, how do we minimize risk as much as we possibly can to make sure that business decision isn't putting the business at risk, right? And so the types of things that you've already talked about, making sure that you use VPN, limiting access, depending on where you are going, making sure that you are assumed compromise — take a zero-trust approach to it — and then put in place the things that will keep you safe. Even if you do get compromised. So things like encryption and multifactor are critical in those areas.

Gene Marks:
Daniel Clayton is the VP of global security services and support at Bitdefender. Daniel, it's bitdefender.com, correct? Just want to make sure I get the website, right.

Daniel Clayton:
Correct.

Gene Marks:
That is great. Hey, thank you very much for joining us. Great advice. We'd like to have you back in the future, as this topic is going to continue to be a big priority for businesses forever. So we appreciate what you're doing, the work that Bitdefender is doing, and thanks for your input.

Daniel Clayton:
I feel the same way, Gene. I appreciate what you are doing as well. I've been doing this a long time and you go back five, six years, and people weren't paying attention to security. So it makes me happy that someone is willing to listen to us, and that companies, you know, from Mom-and-pop companies, all the way up to the biggest companies in the world, are paying attention now.

Gene Marks:
Well you know, just as a final word on that, you read about the big headline cases of companies get hacked at the Department of Defense or whatever. I know, we have about 600 clients in my own practice, and I have dozens that have gotten hacked, that I know about. And small businesses don't tend to talk about that to the media anyway, because you know, it's embarrassing. So it's a big issue among small businesses and we all have to be prepared and man, you get attacked, you can be shut down for days or even longer. There are some catastrophic stories that are out there about businesses that get killed by some of the malware that's out there, so you got to be careful. So Daniel, thank you. Appreciate your time. Thank you, guys, for listening.

Gene Marks:
Do you have a topic or a guest that you would like to hear on THRIVE? Please let us know. Visit payx.me/thrivetopics and send us your ideas or matters of interest. Also if your business is looking to simplify your HR, payroll, benefits or insurance services, see how Paychex can help visit the resource hub at paychex.com/worx. That's W-O-R-X. Paychex can help manage those complexities while you focus on all the ways you want your business to thrive. I'm your host, Gene Marks, and thanks for joining us. 'Til next time, take care.

Announcer:
This podcast is property of Paychex incorporated 2022. All rights reserved.