Matthew Todd
Hi. My name is Matthew Todd, and welcome to Inside the ScaleUp. This is the podcast for founders, executives in tech, looking to make an impact and learn from their peers within the tech business, we lift the lid on tech businesses, interviewing leaders and following their journey from startup to scale up and beyond covering everything from developing product market fit, funding and fundraising models to value proposition structure and growth marketing.

We learn from their journey so that you can understand how they really work, the failures, the successes, the lessons along the way, so that you can take their learnings and apply them within your own startup or scale up and join the ever growing list of high growth UK SaaS businesses. Hey, and welcome back to the podcast. I'm pleased today to be joined by Guy Golan, CoFounder of Performanta. Great to have you on the podcast.

Guy Golan
Great to be here, Matt, and thanks for having me.

Matthew Todd
No problem was so looking forward to the conversation and let's kick things off. What is it that your business does?

Guy Golan
Performanta is a managed security organization that basically focuses on cyber safety through what we call a cyber safe platform that we built, which is a unique, XDR solution that provides clients with a safe mindset, as opposed to just investing on security not seeing the value. So a

ll in all, the organization what we do is we keep clients in the shortest possible way. Free from harm from any potential headaches and try and lower the risk and limit the if something of that nature is is due to happen.

Matthew Todd
I think that makes sense. And one thing that stood out to me when looking at your website was the mention of cyber safety versus cybersecurity so I'd be interested to hear you elaborate on that a bit more and what you see the differences are.

Guy Golan
I'll try and address that both empirically and philosophically. So from an empirical perspective, because that's what people will probably realize and will resonate with them very quickly, is the sense that we spend more money on cybersecurity than ever before, we employ more people in cybersecurity than ever before. And yet, the cybercrime is greater than ever before, which means something in the equation of securing ourselves versus equals means I am safe while I am in perfect condition is far

from the truth. So the upside of it from that perspective is people live in a state of safety or false sense of security, but they're not really safe. The reality of it, if we check it in that way is to say, check most companies that were hacked, they were actually compliant. If they are compliant, that that means that basically, compliance is not enough. From our philosophy, compliance is the bare minimum one should be doing there's much more beyond that.

From from a philosophical perspective, safety is a mindset and is a mindset that needs to be backed by a true feeling of comfort. And if you try and really think about what safety is through and through, then safety is the actual definition of organizations that can continue with a planned routine uninterruptedly. So forget about a company think about an individual. If you know, for example, that you will be fired or there's rumors about retrenchments, the first thing that will come to your mind is, am I safe. And if you do not know if you're 100%, safe or not, what you then do is you start speaking to people asking questions, spending time on the internet looking for another job, which means all of that deviated you from your job, which you're employed to do. And that means that your daily routine was interrupted, that means that you are unsafe.

So organizations live the same level of mentality now. The reality about why they are safe or not safe and how to bring it to cyber safety position is probably this is the whole being of what the format is about. But that we have to also add a little bit of convergence or to put convergence points into the discussion. One is that we are in more digital transformation than we've ever been before. And we do not realize as human beings the impact of digital means on our life, and our physical life. So the reality is, if people don't realize that, I ask them three questions just to make them realize even further and I say where do you carry more cash? In your wallet on your debit card? Where do you have more photos on your in albums on your phone or in albums on the shelves? Where do you have the most up to date data of your contact details? Is that in Rolodex or on your phone?

Elon Musk says something quite interesting is that actually phone has the perfect memory of a human being. So the reality is that we forget about it, but the phone is being used by us. And more importantly is what do we feel when, for example, the money is evaporated out of our bank account? What happens when we can't find photos, all those affect us physically and emotionally, which are all physiological impact. Same goes with organizations, they are impacted in digital means, sometimes they do not understand or they fail to realize that it will impact their actual physical existence.

Matthew Todd
Yeah, absolutely, I can see that perspective. And I've seen it a couple of times when, you know, particular Amazon data centers go down or what have you. And then suddenly, a company realizes how many services they have that are directly dependent on the thing that went down on the data center, they also start to realize how many third party services they use that were also reliant upon those same data centers and connections as well. And I have seen organizations almost grind to a halt, albeit for a relatively short amount of time, but it was still a matter of hours, you know, at the time, so it's pretty serious,

it is serious. And the impact is even more serious when people just apply their mind to it, because you will have two extreme type of border directions, one that will say, I don't really care, I've invested some money.

And the other one is a completely paranoid board. And both are actually finding themselves in a position that they're not sure that they've invested the money in the right place to get the right outcomes, which are driven by potential risks. I hear over and over again, people telling me that we need to educate the board.

And I say, no, we need to educate individuals, that's fine. But the board, if you're, for example, in shipping, or you are in logistics are in banking, and you want now to open a factory of 100,000 square meters, the board doesn't need to be expert, they need to get the right information to make an informed decision.

Guy Golan
What we see is that the board is inundated with data, but not necessarily with meaningful information to make the right decisions. Simple example, there is what we call, there's a graph that shows risk reduction versus the effort that you're going to put in place. Now the seesaw is really trying to get more funding most of them for the right reasons.

Now, if you look at where most of the money goes, it goes for what we call governance risk and compliance, which is to make sure that the company is compliant, so they can continue operating the way they operate. But if you look at that graph, to have a proper GRC. It's a momentous effort. But the risk reduction is very small, which means most of the money goes to a place that you will spend it on being compliant, but actually not reducing the risk. And yet the board when you come and say I want more money, they will say that we just gave you, we give you about 10 million pounds.

And why do you need some more, but if you show the board the information to say most of the money actually goes to cover you, as opposed to actually being safe. And if I just get another 300,000 pounds to do something that is very high risk reduction is very low effort, like batch management. All of a sudden, the discussion becomes more valuable.

Matthew Todd
Yes, there's much more aware model of looking at that, that risk. Because I imagined that yeah, a lot of people will see that, yeah, if we're compliant, we've ticked the box. I've done my job. It's not my fault if something goes wrong from from this point. But yeah, I can see how there would be a number of other investments once you've kind of reached that bare minimum kind of foundational level, I guess.

Guy Golan
Indeed, indeed. Now, if you take that statement that I said, and take it one step further to the board and say you need patch management, because then your ATMs cannot work, or your machines in the factory will not be able to potentially operate as they should. And the potential loss per day is 20,000 or 20 million, whatever that number is, the board can make even more informed decision.

Matthew Todd
Yeah, absolutely. It's about quantifying the the impact of that, isn't it? Its that, you know, classical risk reward. You know, what is it worth to protect against a significant loss like that?

Guy Golan
Correct. And the challenge that I see in our world is that we are doing a secure score or a risk score, but it is so detached from the business. Like you get a security score or risk score of eight, what does it mean? What is the real impact to the business? I used to do that exercise with, with my children. And it's funny, I've got four of them, and you just put them in one room and you say, seven, and you just keep quiet for a month and you say seven, and then all of a sudden you hear my daughter saying eight, and then my son goes 12 and then the other son goes 52.

And eventually it ends up with millions. There reason for why it even happened. That's what happens in board of directors when you give the wrong information because you say, seven. Some people say seven is terrifying. Some people say seven is nothing. Yeah, it's very subjective, it's meaningless.

Matthew Todd
Yeah, you got to take that and apply that to actually how the business operates. And I can imagine that different risks, if manifested, would have different impacts in different parts of the business, which would therefore, you know, result in different losses or different periods of unavailability or whatever that may be.

Guy Golan
Correct. You did.

Matthew Todd
As a business, I can imagine, especially in your domain, the risks that exists, are changing in an ever increasing pace as there is more technology adoption, as you mentioned before, that imagine that the sophistication of attacks as well as also increasing, so be curious to hear how you've, as a business managed to kind of stay on top of that in terms of your own execution, but also client education as well.

Guy Golan
Brilliant. At first, let's understand that attackers are behaving like water, they always look for the path of least resistance, and they go through that path. An example, one of the banks we did in an exercise, about fraud, about loss to fraud, and we came and said, your internet banking is not good, you will be hammered. And the head of fraud at that time said, I'm not really worried about it right now, I'm more worried about fraud, credit card fraud.

And the statement is true, is because your credit card fraud is the easiest one, it's not mature enough. But once you move into another layer and your credit card is well protected, you're going to be hit very strongly with internet banking platform. So I got a little bit of a weird eye when we made that statement as a company. The truth behind that is that basically, I can't remember but few years later, three years later, that bank was hit by the biggest fraud on internet banking that they've ever known. Sothey took the progression, the natural progression of maturing the credit cards, but they didn't take the natural

progression of maturing the internet banking, because at that time, it was not a risk and they forgot about it. Now,that basically means that attackers are looking at, if they can get something very easy, they will do it like in impersonation of smaller organization, change your banking details, we saw a massive influx of those SMEs. On the large organizations, we see a big change from an actual ransomware in its traditional format, which says, basically, I will take your information, and I will encrypt it. And if you don't pay me millions in the form of Bitcoin, I will then delete that information. Attackers realized that actually, they can do much better than that. They just copy your information, don't they don't even encrypt it anymore. And they have got few screenshots. But obviously, we can't show them. The attackers are running a campaign on the dark web. And they say, inflammation of this and this mining company, or this in this manufacturing or banking. I've got three and a half or 3.5 terabytes or seven petabytes of information, whatever that is, this is what the information is. That's what I've got. And for the record, I'm about to publish it in two weeks time, guess how much use you're going to get to actually advertising themselves. And eventually, two weeks later, they just put it down on the dark web with a price tag. And then the highest bidder is the one winning it. So there is an evolution. Not only that the attackers today, funnily enough, are having marketing people not just marketing abilities, marketing people, while they're running it as a business as opposed to running it as a bunch of people. That is an evolution beyond the syndicates or the way that they used to work just as you know, as the underground type of activities.
So the evolution was there were some
people that did it for fun, then they didn't for money, it stuck there for money. Then they collaborated with governments and now governments are doing it for money like North Korea, like China, like Russia. There's a group called Akira that the basically belonging to the Russian government, and that making money is as a result. And then you've got the evolution of it is which is to take the technology and say, What can I do at the least amount of effort to organization. Most organizations are not as mature as they should be to attack a bank. Yeah, they've got armies and you can make really much better and good money by attacking non banks or non financial service providers. And you can get much more than that. So the evolution is both on the attacking methods, on the maturity of the attacker that they become a business. And about the backing that they've got, which is a government backing behind in some cases, obviously, we can't generalize. It puts always corporates, as in corporates can be fortune 1000, corporates, that could put them in the backfoot, because they're not as ready as they should be. And they're not as mature as the attacker is. As before, what we do from an engagement perspective, we first try and explain the situation. It's sometimes it falls on deaf ears. And the majority of the times it actually creates and resonates very well, with organizations, especially when we give examples through, what we try to do is that's where the safe platform is, we developed tools and means to provide information, data and information and highly contextualized information to C level and to the board. So they can truly understand what's happening in their environment. The reason why we do it that way, is because most organizations, they don't want to hear about what happened to the neighbor.

But after about an hour, they will probably forget about and go and have their lovely dinner. But if it happened to them, they're going to be far, far more alert than what they should or would've been. So if you start showing them what's happening in their environment, and then attach it to the methods of attacks that others are doing in their industry in their geography. So you slice it according to a geography and according to industry, you start getting a lot of insights, and a lot of resonated statements by the C-levels, and the board of directors.

So this is what we normally do, to try and get that in place from aligning ourselves into the attackers, I just want to make a statement, the reason why cyber security or cyber safety exists, is because of us. We are all very lazy individuals, we all prefer doing a lot more with a lot less the phone, the smartphone changed our world, almost entirely. And because of that organizations are providing us more capabilities to deal with them.

And that means that they're all digital, that digital has made life a lot easier for the attackers because they don't now do need to break into a bank to steal money or to steal gold medals or metals, they now just need to click a button. What we do is obviously, we've got a very strong r&d team that in a threat intelligence team that really checks what's happening. And we try and categorize it, whether it is something completely new, or it is part of the existing methods, but a new symptom to it. Most of the attacks actually new symptoms, but they're not really new attacks.

So they're using an old like 60 year old methods. But now, because there are new devices and new exposure to the digital world, they just find a new way of doing it. But the methods haven't really changed throughout the period of time. And that's what we do is part of the process.

Matthew Todd
How does the the platform then, you know, help them become more safe on ones flagging those up?

Guy Golan
Oh, that's relatively easy. So if I go with a platform, I can give you a lens that you will understand what I don't know, you don't need to understand cyber what you need to understand your business. And I will give you information that is ready for you.

As an example, if you are in charge of a factory or medical service, or at the ATMs or point of sale in the banks, whatever it is. And I show you that we see a reduction in performance and potentially a stoppage in performance due to a potential risk that is rolling as time goes by because the attacks are doing one thing today zero day, or very minimal. It's mostly advanced, persistent threat that happened throughout the years. And through the weeks, months and years.

Then all of a sudden, the platform is capable of providing that level of lens. And as such, not only that, that we have an understanding from the C level or the decision maker side, we also give some ideas of what the right action should be to reduce to mitigate that level of risk that we are now you know, facing.

So that is what the platform is so unique. Think about the following if you know that there is a car crash a mile down the road. And if you know that Waze will tell you via left and just bypass that and then you continue driving to your destination. All of a sudden, you might have had two minutes detour but you didn't really stop in a traffic jam for two hours, three hours, and your day was completely ruined. Our job is exactly to achieve that in the cyber world and the platform, the safe state is doing exactly that. We we can find ways and means for you to operate while you're under attack. Or if you are before an attack, which means a mile down the road, there might be an accident. But we have a way to actually say

reduce your speed, stop for a bit. Oil on the on the floor, things of that nature, all of a sudden, you are, you're much, much better and well prepared for it.

Matthew Todd
Yeah, more aware and more in control there. I think it's really interesting to hear that perspective, that mentality and particular view of, of cyber safety. And, you know, when it comes to perform Anta as well, so you've been running for 13 years now as we record this?

Guy Golan
Correct.

Matthew Todd
Talk to us a little bit about the growth of the company itself, you know, how did how to think startup and develop? Our audience will be interested to hear how it was at the beginning, and also how you've managed to successfully grow and adapt the business and innovate as well.

Guy Golan
So we started on the first of May 2010, with nine employees from day one and few very loyal clients that we brought through our previous engagements. But the whole idea was from our perspective of the time, and we'll show you that we've evolved, as well. We started by saying, we need to provide clients the journey, they've got something called solutions, and many do box dropping in some do solutions, we want to provide a journey.

When we analyze that we saw the journey has consulted consulting, technology, and services. But at that time, he was very minded to doing technology and consulting services, were serving the objective of selling technologies. That's how we started after.

And then a few years later, one of my business partners said that he wants to learn the offensive world. So sent him on a training and he came back few months later, and he said, Whatever we know, doesn't really help anyone, we're just making money, but we're taking money from from people. And I took a huge offense to that, because that's exactly what we don't want to do. And when he spoke to me about it, and he showed me that the eyes were just lit, we are literally doing the wrong stuff. So it was more about Okay, let's move the business from selling technology into more managed service. Let's help the clients truly by providing them our experience and expertise and share that with them.

So in 2013, we opened a SOC, it was a terrible, terrible SOC, we, we had so many mistakes that we've done on the way mill and like we have deep tissue scars that we've done throughout the way. In 2017, we realized that even the sock in its current format, the way of detecting things through the sock are just not enough. So we started attacking organizations, and almost reverse engineering how we need to defend against those attacks. And that brought us in late 2017, early 2018 with the concept of cyber safety, of bringing that mentality to the world and to companies. And that also changed the entire way that we do business.

So for example, the company grew from nine people to 200 people from, you know, a very small amount of revenue to over 14 million pounds around the planet. But if you look at the combination, we sell much less technologies than ever before. We do it for clients, if they need to sell power knowledge, and we sell a safe solution for clients, we try to bring them to the point that they will not face a situation of being attacked, we can't guarantee that. So when they are attacked, we try and bring them very quickly back to the daily routine. That's the composition of what we did. So it was a painful thing. And you know, it's quite interesting that you asked of Matt, because it took us three years of painful day in and day out to convert the business, from a technology mindset to a managed services mindset.

I'll give it as an analogy. Imagine Steve Jobs comes to his investors, to his employees. And he says, I've got something that we'll be able to run 10,000 songs on it and the guys will come and say, but there's no hole in it. Actually, there are not two holes in it. And where's the tape? And the guy said no, no, you don't need any of that. We need just to have you know this box. So in people's mind, they're so fixated about what what we're selling technologies with technology here. I say, Well, you don't need to sell technology the customer already has those. That mindset took a while for them to change.

Today you speak to most of our employees, they will say, we are a managed services organization, selling technology is a byproduct only if the client wants, you're not making money on that. So it's 13 years of evolution, not only because of what we did, right and wrong is because of how the market evolved. We were very lucky to to understand it as quickly as possibly can. And the other addition is that we saw Microsoft, for example, changing ours in 2017. I met with Satya Nadella in Redmond, I was privileged to have him like for very few minutes meeting in the r&d centers. And they said that we're going to invest a billion dollars on cyber in 2017, we have many, many people laughed at it, we saw the tsunami is coming we saw the wave coming. So we aligned ourselves with Microsoft. And today we are we enjoy that wave of making Microsoft clients much safer than they would have been without us.

Matthew Todd
I think that speaks to to what I often talk to people about which is, you know, selling to the problems that the customer is experiencing and the challenges that they're facing, rather than, you know, trying to morph the solution that you want them to have into your view of their problem rather than, you know, authentically, you know, aligning yourself to their problems and challenges. But I imagine that must have been a significant decision to make, but also to execute as well. Because I see a lot of people might say, oh, you know, we should head in this direction a bit more we should emphasize in this particular area, etc. But to actually commit to that, and potentially lose some revenue streams that you've already got must have been been pretty challenging to put off.

Guy Golan
We lost quite a lot of revenue streams as a result. We were very resilient in the induystry to compensate that we had a few years of cash being burned. It was a hard it was a brave decision. But we were you know, we had the grit, we stuck to it through thick and thin. The interesting thing is that throughout the process, we had many companies that said let's buy perfomance or you know, you're doing something interesting and and we thought it's the wrong time. One of those is a close friend of mine today that was the CEO of one of the largest system integrators companies on the planet. And he basically, he said, You know what, if we don't buy you, we're going to build it ourselves. And I said to

him, good luck.And he said, as to why you're saying that I said, because at the end of the day, you will be as good as your sales team will be. And if your sales team are selling a blade system and networking, and they're doing the sales cycles, about three to six weeks sales cycle wealth, cybersecurity is nine months sales cycle. Even if they're not the best intentions, they will always it's almost like the endorphins. It's like it's like a drug, you want to sell things quickly. Because you know that you're going to get the influx of cash, even if you wave in front of them a 10 times more commission, they will prefer doing that quick cycle and small reward rather than long cycle and big reward. And they tried. And they closed that department actually the CEO for that division now works at Performanta exactly for that reason.

So they tried, they really try very hard, but we can't change the mindset that easily just by you know, dangling the character. There's a big cultural change. There's a big the rule of six I call it you have to repeat yourself six times to really start effecting change the energy for that, and most large organizations lack that energy.

Matthew Todd
And to to make such a decision and be committed to it as as well as to turn down you know, potential sellers why you must have a pretty big a pretty significant pretty meaningful vision that's that's driving you. So what is that that vision behind performance? What are you wanting to become?

Guy Golan
So so the first step of the vision was to become a safe platform and we've got it so we are a platform. And the real vision the big vision of Performanta is that How amazing would it be? If we can reduce the costs of cybersecurity quite substantially by providing very quick detection and very effective detection that will will basically upset the current measurements that people are working on and provide a better level of safety simple example, if we can tell that an attack is going to happen on machine 114 and 2175. Why do I need now to patch all machines, or to defend all machines?

So I had a discussion funnily enough with with the head of immigration of one of the countries. And I said to him, how many people work for you in border control? And he says, across the board, let's say 2000. I said, why can't you employ 10 Is the well, I don't have budget for that. So okay, so this is a budget constraint. The reality is that if you know that aircraft land during the day, and ships arrived during the night, and you know, that pedestrians cross during the late morning, in the early afternoon, you can start funneling your staff to defend your borders in a smarter way.

If we can, in our world, we can truly create a world that is adaptive, and mobile, and we can defend in every hour against potential risks and attacks, as opposed to doing a theoretical exercise, we're going to reduce costs, we're going to increase the maturity and businesses will be able to operate in a better way. That is a big dream of mine.

Matthew Todd
That's a great vision to have. And certainly by the sounds of how you've been able to scale the business, you've been pretty true to that the path that's gonna get you there. And in terms of that, that

growth, you mentioned you now 200 people, you know, how do you manage to successfully scale an organization to those kind of numbers and, and have that level of alignment within the business?

Guy Golan
Okay, so first of all, first in I've made it a commitment, up to 300 employees, my job is to remember every employee by their name, and know a bit more. And I live to that, it's important to me to know every employee of mine to know a bit more about the family, about who they are about their hobbies, and so on. And I don't have someone coming to me with a paper. And just before I meet with someone, they give me the brief of that individual, the scaling was a painful matter. Just because when you're a startup, you, you're used to doing everything as a team, and quickly everybody's jumping in the ball. When you grow, you realize that everybody has a role to do now, that's when genuine accountability comes to life matters, you have to really trust the person to do what it is. So there's massive amount of processes that need to be built as part of scaling.

And we've been doing it ever since we grew over 70 people, and we're continuously building more and more processes to get us up to 300 or 400 whatever their requirements will be as a working organization. So the processes definitely the place. On the people side of it, put in place a massive amount of training and learnership and growth. I cope with a learning culture. So it's everybody how they teach one another to grow. And other technologies we've invested massively in automation, and making things more effective. Why do we need to do the same thing twice? Or three times? If I can employ you to recommend for me how to never repeat it again?

Matthew Todd
Yeah, absolutely. I think automation is, yeah, very important. I think there are capabilities these days, you know, you can do a lot with automation, that that wasn't possible even just a year or so ago.

Guy Golan
Yeah, I'll give an example. We log 1000s of tickets on a daily basis from our clients as part of managed services. Those were highly manual. Today, 90% of those logs are completely automated. And if that those tickets are completely automated, and then 10% are being dealt with higher level people that can grow and can mature, and they can contribute. So the rule is try and take the remaining 10% and reduce that even more by applying more effective and automated means to do it. And that's where we obviously takes much longer but then you start utilizing your level to high level individuals in a much better way.

Matthew Todd
Yeah, no, absolutely. And one thing I know we've talked about us as well before the actual recording today was you know, when it comes to that level of growth, how do you do that in a way that is healthy and sustainable as well you know, rather than just you know, guns out, let's just try and get as many sales in a short timeframe as we can, you know, so how do you approach that, that growth for the long term perspective?

Guy Golan

Okay, so first rule, and it's almost like a biblical rule is that we are driving client centricity client is the most important thing for Performanta. And that means that we cannot make concessions to impact client service, the service declined, the quality of service declined in any form shape. And that means that if we are limited, because of any reason whether we've got a big event or incident or we just get too many clients that are on boarded, we'll have to lower down and say, Guys, we can deal with X amount of clients per month, we can't deal with the rest. And then we sit around the table, say, how can we grow it two fold and do it gradually.

So instead of going like, you know, just jumping at it with all the excitement, all the energy only to find out six months later that you pissed off everybody around you. And you lose your reputation because of the quality of service. We do it gradually. But we do it first, responsibly what we do today, I think more aggressively than we could then we did it five years ago, because of the tools that we built around through the tools that we built allow us to ingest much more and many more clients and onboarding more clients than ever before. In the past, we could have done one every few months now we can do quite a few every month. So it's also about the progression of the business.

So we were trying to be as honest with ourselves and as honest with our clients, and being transparent with him. So we never faced a situation that would jeopardize the quality we provide to them. Because we are running after more and more clients and eventually it will be a losing game for everybody.

Matthew Todd
No, absolutely. I think that's really interesting. Especially ways you can use technology to decrease the effort, but still keep that quality at the same level. And, you know, curious, how do you how do you measure that is that surveying clients do you have other metrics that are kind key ones for you to keep an eye on that quality of service.

Guy Golan
So there are a few few ways it's not a single way. So it's few ways. First, we do what we call this promoter scores, which is the client vouching for Performanta we try to do it every six months.

Secondly we've got service delivery managers that engage with the client continuously. And the service delivery managers speak to the client and raise anything from that.

Thirdly, we've got on the commercial side, the account management that also checked out.

Fourthly, we've got executive sponsorship, so all of our clients have executives, anything from a gap up that need to meet at least on a quarterly basis with a client and check up on them and see how things are going. And the last one is obviously you know, feet on the ground, our team on the ground and giving us the feedback about what's happening if they hear and good word of memory.

I believe we've got a very good positive relationship with our clients. So we can hear the good, the bad, and the ugly from them. And there's always good, bad and ugly. So let's let people not fool anyone here that it's not a picture perfect all the time. From our perspective, sometimes we hear amazing feedback.

And we get that and sometimes we hear less of it. But at least it's the client feels better to talk to us about it. I will say that I'd rather have a complaining client, then a nonreactive clieny.

Matthew Todd
Yeah, absolutely. At least they are engaging with the product and willing to provide feedback in that instance.

Guy Golan
Absolutely. One of my employees gave Performanta the name the purple tribe, and it stuck. And clients enjoy using that. And they feel part of the of the tribe. So from our perspective, it allows us to have a genuine relationship between them and us asking them to build something that is truly great. And it aligns ourselves into their objectives for what they are at that point in time. And that quality that we check. So we are taking the words on face value on one hand, but at the same time, what we do is we also try and check, you know, from different sources, how it is just because we want to be do better for our clients.

Matthew Todd
I can definitely see that client centric mindset mentality, carrying through everything that you describe in terms of how you operate in terms of how you've scaled the business as well. And one thing I'm curious about, as long as that, you know, the world of working is, you know, has undergone quite a few changes over the last few years. You know, a lot of people obviously forced to work remotely and then certainly preferring to work remotely.

And now we're seeing you know, people not quite sure where they should be working in organizations, not quite sure where their people should be working either. But from a cyber safety perspective, I can imagine that they're, they're suddenly facing a lot of challenges. Be interested to hear your perspective on on how the workforce is changing the impact of that on cyber safety.

Guy Golan
Yeah, first, we have to understand that the workforce is working or any of those decisions are working like a pendulum from one extreme to the other. And eventually it sits somewhere in the middle of it. So like we see far more hybrid working nowadays than then A year ago. Some come back to the office. Some people say twice a week, some people three, some people are really exaggerating, and going five days a week, which I think is a bit unrealistic, especially when you go to the office and we are engaging with teams meeting throughout the day.

So from a cyber perspective, it's the realization that people selling before the perimeter has died, I just say that the perimeter still exists. But you also have new perimeters, and every person is an island. And they have to be protected in their home environment through the work machine, and if they do work, not work machine like a cellphone.

And if they do it on a network, that is not that doesn't belong to the office, which always is the case, if you work remotely, then what are the elements of defense and detection you need to put in place to ensure that these people are protected? Let's not forget, majority of the people do not cause damage,

because they are malicious, just because they do not know. From that perspective, our role is to try and be the bigger brother, not in the sense, the bigger brother is watching. But the more adult in the room to help them do their job in a sustainable way, while they're not in the office.

The reality is this, if employee doesn't want to work, no matter if they are in the office, or at home, they are not going to work. If an employee wants to be malicious, no matter if they're in the office, or they're at home, they will be malicious. It is about us putting the right tools to enable them and at the same time to monitor if they're doing something wrong.

Matthew Todd
Yeah, absolutely. It makes a lot of sense. And I've seen, you know, heavy handed organizations get that wrong in the past, I won't name them. But I've been working on on client sites before you try and access, you know, a website that says sorry, this is blocked under the category of productivity, use them. Oh, sorry, I was only trying to be productive. At the same time, there are many other mechanisms for you to get data off of those machines that they almost force you to use that are probably less secure than than using, you know, a quality services,

Guy Golan
Exactly. So I have to say this, to go and work on, can you fool the system and find tools that will prevent fooling the system, the first 80/20 rule will be fine. But if you try and push beyond the 80, you're going to spend a lot of time a lot of money in a lot of effort and without necessarily the results that you want to put for yourself.

So the element is about, you know, engaging in employing people that, that, that really care for the business. And you can see that you know, so I would encourage organizations to really check if people are really working while they're at home.

And I'm not talking about the take 10 minutes just to help, you know, the spouse do the washing or the drying, I understand that we'll go for half an hour to the shop because they forgot to buy something that's part of the perks of working from home. I'm really talking about people that deliberately do not work there almost like as being told the quiet quitting.

Actually, we found one of our clients, their employees developed on the laptop, basically, artificial fingers that that basically click on there on the keyboard, just because they realize that they're monitoring clicks, whether these people are working on that. That to me, is the game lost already. If you get to that point, both for the employees and employees, the game is lost.

Matthew Todd
You've acknolwedged there's no trust at that point, haven't you? Surely?

Guy Golan
Exactly. So I would say, let's put the security in place. Let's put the controls in place. Let's monitor that. And on the way, let's also try and give strong, positive reinforcements to employees. But they are doing a good job. I haven't seen one case, nowadays that people say, Oh, you send this information in such a

protective way. Well done. Or you, you operated your phone and you didn't click on that link, continue doing that you're keeping our business safe from any harm, that level of positive reinforcement is lacking. Because we always try to focus about the negative, but actually, it is much more positive that can really change behavior. And that is to me about 50% of keeping organization safe.

Matthew Todd
Yeah, absolutely awesome. And it always, always comes down to the people doesn't it.

Guy Golan
I always say the people the the tale, about the frog and the princess. So, in fact, when the princess kisses the frog, so the frog should turn into a prince. Just like Shrek When the prince is kisses the frog the princess turns into another frog because frog is people in the princesses data. People ruin data, no data rude people.

Matthew Todd
Yeah, absolutely. I think that's really a really interesting perspective. And you know, thank you for for sharing that, and you know the other things as well. I think before we we do wrap things up, is there anything else that you'd like to share with our audience, either related to cyber safety or in terms of growing a business. Are there any other lessons that you you think they'd find useful?

Guy Golan
Yes. So I would love to first from a cyber safety point of view is, if you're a lifestyle business, which means it's all about making money, that's all fine. But please allow us to do our job and not creating confusion in the market, because the market is confused enough. And there's lots of snake oil already in the market.

Second is that if you're taking your business very seriously, just ensure that whatever is being done is done for the value of the client, and being focused about clients interest in because that, again, will reduce a lot of the noise. Right now, it's a national and international level of effort that we must reduce the noise created by different opinions, as opposed to genuine opinions that can create a synergetic and better future for all of us. That's from a cyber safety point of view.

From people that want to grow and scale their business, I would say the easiest possible way. You're very welcome to do it. Make sure that whatever you think you'll be doing, you will be doing when something happens, start doing two steps before that, because whenever you plan to do it, it's already too late.

Matthew Todd
Interesting, thank you for for sharing that. I think the big takeaway is clearly that customer centric approach and a willingness to be brave and committed to that and have that long term vision to carry that off. And that that creates a company culture that creates a business that surely can serve their customers in the in the best possible way. So thank you very much for sharing that really, really interesting conversation and definitely interesting to dig into more of those cyber safety elements as

well. And I'm sure they'll become more and more relevant over time for many people that are listening to his podcast as well. So yeah, thank you for your time today. Appreciate it.

Guy Golan
Thank you, Matt. Really appreciate the time and I'm glad to be here. Thank you.

Matthew Todd
Thank you for joining me on this episode of Inside the ScaleUp. Remember for the show notes and in depth resources from today's guest, you can find these on the website insidethescaleup.com. You can also leave feedback on today's episode, as well as suggest guests and companies you'd like to hear from. Thank you for listening.