EPISODE 1293

[INTRODUCTION]

[00:00:00] JM: SOC 2 is a security audit to prove that SaaS companies have secured their company and customer data. It's often considered the minimum audit necessary to sell software. HIPAA is a federal law regulating how sensitive medical information about patients must be handled. ISO 27001 is the global benchmark for demonstrating your information security management system. What do these three things have in common? They are all security standards that companies need to maintain and renew to be trustworthy to customers. They also take intense preparation with months of work and hundreds of screenshots to prove compliance with auditors. The company Vanta provides automation tools to monitor your applications and maintain compliance. Fix items on your Vanta to do list, and when you're ready, a Vanta-trained CPA will perform an audit with you. In this episode, we talk with Christina Cacioppo CEO at Vanta. We discuss the accreditation process and the security needs for various companies, and how Vanta is helping keep companies in compliance.

Our first book is coming soon. *Move Fast* is a book about how Facebook builds software. It comes out July 6, and it's something we're pretty proud of. We've spent about two and a half years on this book. And it's been a great exploration of how one of the most successful companies in the world builds software. In the process of writing *Move Fast*, I was reinforced with regard to the idea that I want to build a software company. And I have a new idea that I'm starting to build. The difference between this company and the previous software companies that I've started is I need to let go of some of the responsibilities of Software Engineering Daily. We're going to be starting to transition to having more voices on Software Engineering Daily. And in the long run, I think this will be much better for the business, because we'll have a deeper, more diverse voice about what the world of software entails.

If you are interested in becoming a host, please email me, jeff@softwareengineeringdaily.com. This is a paid opportunity. And it's also a great opportunity for learning, and access, and growing your personal brand. Speaking of personal brand, we are starting a YouTube channel as well. We'll start to air choice interviews that we've done in-person at a studio. And these are high-

quality videos that we're going to be uploading to YouTube. And you can subscribe to those videos at YouTube and find the Software Daily YouTube channel.

Thank you for listening. Thank you for reading. I hope you check out Move Fast. And very soon, thanks for watching Software Daily.

[INTERVIEW]

[00:02:56] JM: Christine, welcome to the show.

[00:02:58] CC: Thank you so much for having me.

[00:03:00] JM: You are working on Vanta. Vanta is a very successful company. And what you do is around SOC 2 compliance, as well as other forms of compliance. People listening have probably heard of compliance. Maybe they have done some work around compliance. And I have to admit, when I first heard about SOC 2 compliance, I assumed it was this thing that had been around forever. It sounds like it's old. It sounds like it's been around forever. And it sounds like it's hard to deal with. It sounds like something that is difficult to deal with. And so my first question is, why didn't this exist earlier? So you started Vanta four years ago. This seems like a product that should have been around for a long time. Why wasn't it around when you started Vanta?

[00:03:48] CC: Yes. This is a great question. So backing a bit, so Vanta is a security and compliance company. The joke, that's not a joke at all, is that we're a security company masquerading as a compliance company. And so got into these compliance standards as a way to help companies prioritize and improve their security. And particularly the way we do that is get them these compliance certifications, that when they have them, opened up new markets, helps them sell faster and ultimately grow their business.

And even though I know that why now question about Vanta is a really good one. Like you said, started Vanta basically early 2017. Why didn't this exist beforehand? I don't actually have a great answer. My best answer, which I find a little unsatisfying, is when you say the word

compliance or SOC 2 to an engineer or product manager, they will generally run screaming from the room. And they'll be like, “Oh, don't you want to work on this fun project?” And they will be like, “Right. What else do you have for me? Can I please work on something else?” Until a lot of this stuff just didn't get looked at by engineers or product people. And I think we looked at it and initially had the like, “Yeah, let's run screaming from the room.” The way you do this is generously stuck in the 90s. Westerners, so you could probably say some other things. But looked at it and said, “Well, can we fix this? Can we standardize? Can we productize?” And sort of went from there. But I think that sort of insight hadn’t happen previously just because folks who, again, have this sort of skill set, usually compliance is not the top of their list of things they want to work on.

[00:05:28] JM: Okay. Now, because I have run screaming from the room for six years since starting this podcast every time I heard SOC 2, I've never asked this question. Can you tell me what it actually is?

[00:05:41] CC: Yeah. Okay, really high level. It's a 70-page PDF that has a bunch of detail, but basically says, “Hey, we had someone who's really rigorous and thorough sit down and talk to us. We explained all of our security practices. We’re professionally skeptical. We proved our security practices to them, and they signed off, and think we're reasonable. So, you, potential buyer of my software should also think I'm reasonable. And if you would like more proof, here's my 70-page PDF with lots of detail on how this whole process worked.” But that's what it is at a high level. I can go into kind of different versions of it. But that's sort of the value it plays in the market, which, done well, I think is actually a useful thing, right? Building software, selling software, there's just more and more concern about data security and privacy. And this is one of the things that underlies kind of Vanta’s founding story is we looked around and we're like, “Okay, are people going to be more concerned about data security and privacy in the future or less? Is this a good trend to bet on?” We said it absolutely more. And then you're like, “Okay, great. Whenever a business buys a software, are they going to go do the full investigation, and audit and make sure the data is handled well, and everything's set up reasonably, and da-da-da-da-da. And is every business going to do that every time they buy software from another business?” And I have a background economics. I like efficiency broadly. A bit of a joke, but like I don't think you even need that to look at that and be like, “I hope.” Not everybody goes and investigates everyone else, because it’s a tremendous amount of time and effort. And so having

a centralized way to say, “Look, one trusted party checked Vanta. Said they're reasonable. So other folks can trust Vanta.” Given the in depth work this person did, I think it's a reasonable system. This is what SOC 2 purports to be.

[00:07:32] JM: Right. Well said. Now, when I look at what you actually have to do, I imagine you go into these companies and are looking at their databases and making sure their databases are encrypted. And you can tell me what else SOC 2 compliance actually entails in terms of boots on the ground. But it sounds like a problem that at first glance looks like a consultancy problem. Like you hire a bunch of SOC 2 consultancy experts. They parachute into a company and they analyze every angle of the company to ensure that everything is encrypted where it needs to be. That pipes are as secure as they should be. How is that a problem that you can productize in a scalable way?

[00:08:19] CC: Yeah. So additionally to your make sure database is encrypted, this is, yeah, one thing you do. And again, you can kind of think of the checks that make up a SOC 2, or say 100 things like that. So, “Are your databases encrypted? Are folks’ laptops encrypted? Do they use a password manager? Are people on-boarded to the right systems and off-boarded to the right systems?” whatever. There are like a hundred things like that. And your consultant point is a really good one. In 2017, when I started poking around here and talk to folks, they were like, “How would you prioritize a SOC 2?” Step one is sort of look deep inside your heart and develop your own security practices, right? Like how do you how do you productize that?

And we heard that. And mostly we're just kind of confused and very naive, right? And you’re like, “Well, I can look deep inside my heart. But I probably shouldn't. I should probably just follow the best practices.” So actually really core to Vanta is a prescriptive set of controls, but just things you follow, right? And one of the first things we did in early product development was write down a list of, “Hey, here's a hundred best practices that we think companies should follow.” And then that became the core of the product. And today, you can add and remove things on the edges. But a key piece of moving it from something a consultant does, to something that's productized, is kind of taking an opinionated stance on, “Hey, here's what reasonable security, and here's what reasonable best practices look like 2021 for a cloud software company.”

[00:09:49] JM: I think four years ago, I did an interview that really stood out to me. And that was a –Or a series of interviews. I did a series of interviews with Stripe employees. I think it was about four years ago. And I remember talking to at least one of them about SOC 2 compliance at Stripe, and it sounded really hard. So I'd love to know how you would direct an engineering team to become SOC 2 to compliance and go deeper on the kinds of tools that you could potentially present to an engineering team that would make their lives easier.

[00:10:23] CC: Sure. Well, first up, use Vanta. No. But more seriously. So the first step of any compliance process, Vanta's side, is to decide on the list of things you want to implement. And no matter what standard, like we're talking about talk SOC 2. But all these standards have really high-level guidance. But one thing we found is the guidance is, in fact, really high-level. The guidance says things like we keep customer data safe. And that's kind of the beginning and end of it. And so it's up to the company to say, "Okay, when we think about keeping customer data safe, we think about encryption and transit or at rest. We think about rules of least privilege around employees accessing it. We think about several layers of authentication for an employee to access customer data," whatever, right? And so the first step of one of these processes is kind of figuring out how you want to define. We keep customer data safe. We're reasonable. We hire good people. And again, this is the Vanta take, but I'm actually biased in that like it was our take that we thought was so good that we put into software was one of the things that has made these projects hard historically for small or large teams, kind of like the ones we're talking about, is the feeling of, "Oh, my gosh, I have to go out and do this giant research project and figure out a point of view on all these things."

And I think here's where kind of same defaults and best practices can really be your guide. And so if you're a company that has, I mean, strong engineering practices and strong engineering fundamentals, you're probably doing a lot of the stuff you'll want to do and need to do. And really, optimistically, some of these compliance projects can end up being fueled or prioritized. Some of what maybe you've wanted to do. So maybe we –Dropbox example. I think Dropbo got to a couple hundred engineers without mandatory code reviews. And then there was some amount of desire for mandatory code reviews, but it actually ended up being a compliance project that said like, "Oh need multiple approvers, for something," da-da-da, that really got the team to make that process change. And so I think, yeah, optimistically, some of these compliance projects can – A team can use them to prioritize and get implemented the best

practices they want. And to kind of look at the project overall that way, versus like, “Oh, my gosh, we have this absurd checklist. Someone's going to come in and make sure we stand on our heads on Tuesdays. And isn't this dumb?” But really kind of seeing these as you get to write your rules, and to write the rules you want. Like use this as an opportunity to bake-in the security practices you actually think are reasonable for a company of your size.

[00:12:53] JM: Yes. You mentioned Dropbox. You worked at Dropbox for I think four years before you started Vanta? Is that right?

[00:12:57] CC: Yeah. Two years. But yep.

[00:12:58] JM: Two years. Okay, right. So Dropbox, of course, has a plethora of security challenges. And I'd love to know if you're – Or to what extent your inspiration for Vanta or your strategy around Vanta was informed by your experience at Dropbox.

[00:13:19] CC: So it was. So I was a product manager at Dropbox on Dropbox Paper. Just sort of their version of Google Docs, an online collaborative editor. I joined the team with five or six people and the product was on launched. So super early. And as we were trying to take it to market, one of our initial ways of getting users was going to the account managers at Dropbox. So kind of the folks who worked with the existing large customers, and just asked them to start giving away our beta. We even called the beta. Just start giving away Dropbox Paper to these customers, which the account managers were very excited about. Because they spend all their days calling up customers and asking them for more money. And I basically went to them over lunch and said, “Hey, can you just have them try this thing?” Anyway, that's how we got our first users on paper until the Dropbox legal team learned what we were doing and got reasonably very upset. Smart people doing their jobs, but they sort of came to us and they're like, “Hey, you're going after all these big customers that have contracts.” And the contracts say Dropbox is secure, and compliant, and pen-tested, and XYZ, and ABC and alphabet soup. And Dropbox is, but paper is not. So you either need to fulfill these contracts or stop doing this like ASAP.

And we sort of didn’t know what the words meant, like do fuzzy PM. It’s like, “Oh, well, how do we do that?” And we went and costed it out and found out it would take us about 18 months to go get SOC 2 and do all the things the contracts wanted us to. And again, we were like five, six

engineers. Didn't have product market fit. We're like, “Are we going to put everything on hold for a year and a half and go do this project like and then wake up in a year and a half and be like, “Well, now, I'm going to go try to find product market fit. Hopefully that works,” right? Like no.

So what we ended up doing from a go to market perspective was took Paper to market with actually blocking access to anyone who had a Dropbox contract. So that was a rough strategic choice. But I think it came from being like, “Look, this is Dropbox at 2014 2015, the height of Dropbox’s power, and it's still takes us a year and a half to go do all this stuff. Like what is going on here? Why is it so hard?” And some of us started to dive in and see like how bespoke a lot of it was and how, I mean, rooted in accounting a lot of the standard was. Not in software engineering.

[00:15:39] JM: What you're describing is a proxy for what a lot of companies deal with, which is a point at which they need SOC 2 compliance in order to reach a new tier of contracts, basically. Like there is a category of customer, which is also going to be some of the most valuable contracts that you're going to be able to close that needs SOC 2 compliance. And beyond that point, I mean, you can be Slack, and sell to startups all day long. But eventually you're going to be selling to banks, and then you're going to need SOC 2 compliance.

[00:16:17] CC: Yeah. And this was one of the things that we actually quite liked about it, is our basic thesis was like, “Look, the pull to get a SOC 2, to your point, is really strong.” It opens up new markets. It grows your business. It takes you up market, right? It does all of these things that are like board level topics where the company is like I want everything I just said. And so the pull to get a SOC 2 is really strong. The process of getting a SOC 2, and depending on how you do it, some of the processes that result can take a tremendously long time. It can feel like a ton of overhead. It can be really frustrating. But people still do it, because, again, the pull is so strong. And so we sort of looked at that, and we're like, “Okay, here's something that companies are going through even though they really don't like it, terrible process, etc. Can we change that so it's actually a net positive to the company's operations and security? And will they go through it even more?” And that was, again, some of the origin of Vanta of like how can we take this hair on fire problem and start orienting it around what it's designed to be oriented around, which is demonstrating the good security practices a company has?

[00:17:29] JM: Jus to pause on Vanta for a moment and thinking more about Dropbox, I think of Dropbox as a company who their core product has been so successful that they have been able to double down on their core product while also experiment with other products. Now, kind of making a second product in a very successful company is notoriously difficult. And I wonder if you have any lessons of innovation around like seeing Dropbox – The span of time you were there, 2014 through 2016. I think that's right before or around when they started the Magic Pocket Project, which I would say has been one of the most successful major projects they've done. Not a lot of people know about it. But this re-platforming that totally changed their cost structure and give them all kinds of future proofing, I think is really cool. But aside from that internal innovation, there're lots of outwardly focused innovations like Paper and Mailbox, the Mailbox acquisition. Tell me about how Dropbox informs your long term product thinking.

[00:18:41] CC: Oh, that's a great question. So I joined Dropbox in 2014. And again, I don't overstate my role or impact. Like I was PM. I was certainly not anywhere near the company's leadership team. So I'm just going to talk about what kind of things I saw. But I think 2014, the writing was a little bit on the wall of consumer file sync and share was going to be offered by some of the major Internet companies, Apple, Google, Microsoft for free. And it accounted for at the time, a tremendous portion of Dropbox's revenue. Kind of still did. And that business was growing. It wasn't slowing down until it was this really interesting thing to watch where, again, there was literally hundreds of millions of dollars at almost an increasing pace being made from this business, consumer files, that everyone was pretty sure would look different somewhere between five and 10 years, but didn't really know when.

And so, again, this interesting time to be there, because it felt like both the business was doing very well. And there was this kind of impetus to try to find a second or third product. And so whether it was –Or actually I think, and this was pre my time. So again, I don't want to take zero credit for this. But I think what they did was they looked and said, "Okay, here's all the files that are in Dropbox. Can we build applications around them?" And so you get something like emails with mailbox. You get something like photos. We made a photo product. You get documents and you get paper, right? And so it was sort of the strategy of, "Okay, files might be going away." But these kind of core primitives are still there. And can we own the experience around those?

And so Paper is one example. I think Dropbox did –So that is a broad strategy piece. I think the other thing that was sort of interesting with some of the new product initiatives at Dropbox were sort of homegrown. So hey, we're going to put a team of four people over here and have them think about chat, or documents, or whatever it is. Some were acquisitions. So Mailboxe is a notable one. Dropbox Paper, the core of that actually came in through an acquisition of a YC startup called Hackpad. And I think it was all just interesting to watch those. I think from a kind of platform engineering perspective, it was really interesting to see the tradeoff. Again, something like Paper, which part of why we had these security and compliance issues is because we were on the original startup's codebase. We were totally separate from the rest of Dropbox, which for the most part was great, because Dropbox at that time was like a 10 year old monolith that had like hundreds of engineers and broken builds, and everything that comes from a large, fast growing engineering organization. We had this startup code base that we could move a lot faster on, but that didn't have the security compliance privacy safeguards. So just that swap.

I think to answer your question about lessons, lessons kind of learned, I think something I've tried to take to Vanta is I think it's actually – Well, twofold. One, really important to build a sort of second third act muscle in the company, right? So even if your first product has product market fit and successful, like kind of no technology company has just survived on one product. And so you really need to figure that out. And it's actually harder to figure that out the longer you wait, culturally, for a million small reasons. And so I think Dropbox has a tremendously, like just fantastically successful first product. Like the true story of you put something on Hacker News and like 10 million people download it, right? You're like, "That doesn't happen," except it happened to Drew. And then it just started kind of printing money and a lot of ways, right? And it was truly incredible.

I mean, it is a multi-billion dollar business based on that. Largely, right? It's tremendously both skillful and lucky. I think one of the things it does push on is they didn't need to develop a second product for a really long time. And so by the time they were trying to build that muscle, it was within an organization that was very good at kind of serving the first product for good reason. But kind of put the pressure on figuring out second products early on.

[00:22:58] JM: What you're describing there with the second and third act muscle, that's one of the most interesting things about the companies that seem to be perennially reinventing

themselves is they have this systematic means of innovation. And obviously, like, as a startup, you don't have the bandwidth to think about that all the time. But keeping it in the back of your mind and knowing that your options are open is really important. I mean, this is no insult to Dropbox, but the name Dropbox is arguably a little bit limiting. Like what are you building? Okay. We're building a place to drop your files. And that's great. It's fantastic. The name Vanta. I don't know what a Vanta is. I couldn't tell you what a Vanta would be if I saw one. So you are you are in –

[00:23:46] CC: It's a llama? Yes.

[00:23:48] JM: It's a llama? Is that what it means?

[00:23:50] CC: No, it doesn't. No.

[00:23:51] JM: What is Vanta?

[00:23:52] CC: It means advantage and finish. It mostly – It was a word we liked. It's really kind of the true story. It's a word we liked. A .com we could get for kind of the price of maybe a small car, but not a luxury vehicle. Some domains cost.

[00:24:07] JM: Okay, so as far as your second and third act strategy, you have some obvious short term expansions to HIPAA compliance, other forms of compliance. But I imagine that the laundry list of compliance things that you can work on has some boundary, right? Where do you go from there?

[00:24:27] CC: Yeah, so I think a lot of this is also when you think about second and third acts of like what at its core is the company doing, right? And so at Vanta's core, we think about we ingest configuration information from all sorts of systems, cloud infrastructure, HR, mobile device management, laptops, like identity providers, and check for configuration and misconfiguration both within a system where all your database is encrypted to your AWS point earlier, and across systems. Sally just joined the company as a new engineer. Does she have access to what she needs to whether on an account level or like SSH keys on her laptop sort of level, right? That's what Vanta does.

And then we can like combine these checks. We can bundle them into something that will get you a SOC 2, or get your HIPAA, or get you name your alphabet soup certification, right? But we can also bundle them into like, “Hey, you're just starting out. I want to make sure you're being baseline reasonable. Like not a doofus, right? What should you do?” And so I think in Vanta’s sense, like you'll see us kind of take the checks we do, I mean, expand them, breath more of them, etc., and then bundle them in various ways. Some around what we call recognized compliance standard. Just like the alphabet soup of stuff. And some around things we probably create at just different price points all the way through.

[00:25:44] JM: Interesting. Okay. Well, what about from a management point of view? How has the expansion into different forms of compliance affected the management structure of the company?

[00:25:57] CC: Well, yeah. I think it has forced us to, I mean, kind of play by our own rules and be a little more standardized, right? The product that we initially built and sold kind of almost up until today was very SOC 2 too focused. We just encoded a lot of assumptions of like, “oh, SOC 2 needs you to do this thing. So that it's written into our code as the thing.” And a lot of the last six months has been pulling back and generalizing, right? And saying, “Okay, SOC 2 wants this. HIPAA wants that,” right? And so I think moving into different standards for us in these different products has sort of been the –Yeah, just forced us to generalize what we're doing and think at a higher level, like think a little bit at all like model and principle and sort of invariant level. And then go and we can – Go to SOC 2 things, whatever, but have those be no more special. Like SOC 2 concepts are not first class citizens of our product today. They used to be, right? Just because it was an MVP, if that makes sense.

[00:26:58] JM: Gotcha. So I imagine there's significant overlap between these different policies. Like I mentioned HIPAA, and ISO 27001, and SOC 2 all have similar constraints? Or maybe are there new things that you've had to build in order to have the compliance protocols for the other domains?

[00:27:20] CC: Yeah. So definitely new things to build, but there is a good amount of overlap. I think when we first started looking at this market a few years ago, we learned that actually the

mapping between different standards, so SOC 2 section 2.2 makes you do this, and ISO annex, whatever, makes you do that. That mapping, that spreadsheet mapping, is actually what a lot of the audit firms think of. It's their IP, which is interesting for a software perspective, right? Because from a software perspective, you're like, “That quite information should be free.” But like that doesn't seem like the most sustainable source of IP or competitive advantage. But it was just, I think, a difference between the kind of services mindset and more of a software scaled mindset.

Anyway, all to say, one of the things we have done behind the scenes is map different parts of these standards to each other, but also take a kind of opinionated stance of, again, these certifications are really high-level, but like, what sort of best practices from software engineering can we apply to them? And then where does it apply across different standards? Yeah.

[00:28:27] JM: So the whole reason for this compliance world is – I should just ask you, I presume that SOC 2 compliance is in some ways about liability protection. So if I'm a bank, and I want to use Slack, I'm going to be communicating very sensitive data across Slack. If Slack gets hacked and my banking chats get leaked through Slack, that could potentially cost my company millions and millions and millions of dollars. Therefore, it's probably really important for me as a bank to make sure that there are some policies in place for making my data safe. For all I know, maybe there's even like insurance that the bank needs to get that's related to being SOC 2 compliant. What does it actually mean? Like if I'm operating a bank, and I'm looking out at the vendor marketplace, and I'm looking for places that are certified with your llama logo that have SOC 2 compliance imputed by that that circular logo of Vanta, what am I actually getting? And why am I getting it?

[00:29:40] CC: Yeah. So if you’re a bank, some part of your organization is like, right, like risk management. Probably lives under the CISO, and they're thinking about risk really broadly. Some is internal. Some is external. But one part of extra risk is vendor management. And I'll try to stop using all the Gartner words, because I know there’re a lot of them. But, basically, someone at that bank is responsible. It's like, “Okay, we're going to share customer data with some of our vendors, either because like, our vendor is Microsoft and we use Office 365. And like there're customer names and spreadsheets, right? Or there's some software vendor –” And we text message our customers. And so we're Twilio and customer phone numbers, whatever it

is. Even if you're a bank, basically impossible today to operate a business without giving some amount of customer information to some sort of software vendor.

And one of the things I think we've specially seen over the last few years is like when a vendor gets breached, the company basically gets breached, even if that's not true. So when Target's air-conditioning vendor, or whatever it was, gets breached, target customer information goes out the window, and target customers get angry at Target. They don't really get angry the air conditioning vendor, right? It's on Target for being like why did you trust these untrustworthy air conditioning people? Also, why didn't you give credit card data to your air conditioning vendor? Separate practices question there.

[00:31:01] JM: This is a real story, by the way, that you're referencing, right? Like, yeah, people –

[00:31:04] CC: Yeah. It's the most absurd of them. Yeah.

[00:31:07] JM: This is the case where, basically, what is it like Target's point of sale systems were hacked through an air conditioning. Was it even –

[00:31:16] CC: Was it air conditioning or something? Like if something literally like humidifier or something?

[00:31:20] JM: Yeah, yeah. Somehow the networks were connected.

[00:31:24] CC: Right. There's stipple on you're like, "Why was that true?" But given it was true, right? This was, yeah, Target's like subcontractor, or subcontractor, right? But Target's customers didn't care. They're just like, "Target, my credit card number, it's now on the Internet. Like I want credit card protection," da-da-da-da-da.

So like this is kind of the world we live in where like even though it's not you, and it's your vendors, it doesn't matter. It's basically you and the court of public opinion and kind of the court of customer opinion. So that means there's someone at these companies saying, "Okay, can we trust this vendor? Air conditioning vendor, software vendor, whatever? Can we trust them?" And

kind of going back to the beginning, right? There's, I mean, really broadly, there's kind of two ends of a continuum of how do you decide that. One is you're like, "Look, somebody I think is trustworthy trusted them. So I'm just going to like chain a trust, believe it." So it's kind of more the SOC 2 stance. A SOC 2 auditor said it was okay. So I'm going to trust them. Or there's trust no one and say, "No, no, I'm going to go really deep. I'm going to show up in this vendors office. I'm going to go interrogate their executives. I'm going to look in their eyes and see if they're reasonable people, right? And what to do?" And then there's obviously a lot of stuff in the middle there. But that's sort of what it is. It's like how much effort is at the bank going to expend figuring out if a vendor is trustworthy? And how much are they going to rely on some sort of third party? Vanta, SOC 2 to auditor, their friend's bank, whatever it is.

[00:32:53] JM: So what happens the day where Target is now buying Vanta-certified air conditioning software and, nonetheless, the air conditioning software company makes some kind of data breach mistake, or some kind of mistake that leads to a data breach. And now the onus is on Vanta. So the air conditioning company comes to you – Well, actually air conditioning company still doesn't care. Target comes to you. Target comes to you and says, "Hey, what gives? What gives?" And you got to say, "Look, we inspected them as best we could back in 2021. But the 2022 data breach was just – It was kind of using outdated compliance certification. Well, I'm sorry."

[00:33:37] CC: Ooh! Yeah. This is good. So, look, this is the way the world works today. Not with Vanta, but wich SOC 2 to audits, right. And without naming names, basically, any company that's been headlined and breached was SOC 2 audited. And a lot of it was like, "Look, they were good when I checked, but I checked somewhere. I didn't checked today, right? I checked six months ago. And so what can I tell you? I think that is –I mean, it's really easy to criticize, but like, "Look, when it's a service as business, and humans are doing the checking, that is close to the best you can do." If you're a Vanta and thinking about Vanta certification, we think about this in a continuous software powered way. And so we don't have this product out in the market yet. But the way we think about that is like, "Yes –" Let's say that a security status page. I don't know if this is quite the right form factor, but it's kind of easy to visualize, right? And we imagine something where a company is like, "Look, this is my security status page." And maybe just like an uptime, a monitoring status page. Sometimes things are up and it sounds like not everything is 99s, or 100%. But because we're checking with software, we can basically provide real time

insight. And so in that case, you're like, “Look, Target.” Three months ago, maybe everything was green. But yesterday, things were orange, right? Because certain security controls were not in place. Your proverbial internet set up a new database where things weren't configured correctly. Like new employee onboarded – Whatever it is, right? Like lots of stuff happens. But I think the real time continuous monitoring piece and just providing dashboards of this information is really powerful. And I think kind of that alone is enough to change a lot of behavior. Again, when you know the auditor is coming in, things will be in good shape. And so there's a little bit of like, “Well, how can we simulate that all of the time in a helpful way to security, not in an onerous way?

[00:35:30] JM: Gotcha. And I still don't understand how much you can instrument this. Like, what are –If I'm trying to – Let's say I want to install an agent. Again, like we don't have to tie ourselves to this form factor. But let's say we have this agent. I mean, this is a very common pattern in like monitoring software. You install an agent on your different services, and your agent does something like watches the latency for all of your requests and responses and can give you information about that. Is there a model for developing an agent that ensures compliance?

[00:36:10] CC: So, there is actually. Gosh! Probably six or seven years ago, I think Facebook open sourced a project called Osquery, which basically just, it helped Facebook used it for their own internal server management and getting kind of metrics analytics performance off of servers in their fleet, and sort of let them query across a large fleet of servers. I think the original use case, again, was sort of monitoring and performance. But folks have built on that project and the queries that are run and sort of use them for security too. So like who has access to this machine? How is access enabled, right? But again, I think the agent isn't as much the point there, or the useful part of the agent is, “Hey, I've got this fleet of machines, and I want to know how they're set up. How do I figure that out in a quick and scalable way?” And putting an agent, running something, Osquery or something else on it, it's one way to figure it out. But I think, actually, the higher order bit there is just what's the state of these machines, right? Who can log into which one? Are strange ports open on any of them, right? Sort of what's going on? And that insight is sort of the first step here. Does that makes sense?

[00:37:20] JM: It does. In fact, we did a show about Osquery not too long ago. There's actually a company around Osquery now.

[00:37:26] CC: Collide. Yeah.

[00:37:27] JM: Oh, I was going to say Upticks. Okay, maybe there're multiple companies.

[00:37:29] CC: Oh, several.

[00:37:31] JM: Interesting. So I don't know how much detail you could go into about that. But like why is Osquery potentially a foundational technology around automating compliance?

[00:37:44] CC: Yeah, so I think a few reasons why we liked it. One, just that it was open source, right? Like no one likes installing agents on their machine. Like no one likes installing software they don't know. That's totally in a black box on it. So just the fact that the software itself was open source, I think helped a little bit. There's still some amount of objection of like what are you running on my machines? And are you going to cost me a bunch of money or slow me down or causing performance issues, right? That's still there. But just having the code open is helpful. And again, the other part, I mean, in some ways, again, you can kind of think of Osquery as just like the way we get an API to bespoke servers, right? If it's an AWS server, we can use the AWS API's to query setup configuration and reason about it. If it's a bespoke machine, Osquery is how we have an “API” metaphorically to what's going on. But that's the key part for compliance, because it's just a lot of compliances. How are things set up in real life? How do you want them to be set up ideally? Kind of your controls? Cool, what's the Delta, right? And so agent technology, Osquery and others, are helpful in the how are things set up realm.

[00:38:54] JM: Yeah, another dimension of this. I don't know if you've talked to anybody about this, but there's something in the Kubernetes world called the operator pattern. So Kubernetes is this newer infrastructure platform thing. And there's this thing called the operator pattern, where you can basically programmatically describe where you're trying to get to. Declaratively describe where you're trying to get to. And whenever you drift off course from that, for whatever reason, the system tries to remediate that. And that pattern has been useful. Anyway, I think it’s a trend.

[00:39:25] CC: Okay. Actually, I mean, not only metaphorically similar, not actually similar, but we really encourage customers to use infrastructure as code tools, Terraform, Cloudformation, whatever, right? But it's, again, sort of similar idea of like declare the world you want it to be. Figure out the configuration you want. Write that down. Go apply that everywhere. And go from there. And then from a compliance and audit perspective, one, you've actually got a pretty good way to reason about like, “Well, in this file, I said I wanted databases to be encrypted. And so in fact, they all are.” And two, auditors really love more than one person doing something. So if you're clicking around in like an AWS console, it's just one person clicking around and like are you going to make a loom video of yourself clicking around and show it to the auditor? Like, that's weird, right?

But if you're writing stuff down in like Terraform file, and then that goes through code review, that gives you two people. And so the auditor is like, “Ah, yes. Jeff wrote it. Christina code reviewed it. Two people saw the change. I like this change much better.”

[00:40:28] JM: Cool. So now that we've talked about what your company actually does, let's go into management a little bit, or strategic implementation. Give me a snapshot for where the company is today in terms of headcount, and how you're allocating resources, and what your prime directives are.

[00:40:51] CC: Yeah. So we are about 80 people today, close to 1500 customers, roughly half engineering product and design, half go to market, moving toward that. Can talk more about any piece of that if helpful. And then from a strategic point of view, the company's strategy is pretty, pretty simple. It's use what we call recognized compliance standards, SOC 2, HIPAA, etc., to build our product, our technical capability, and our kind of brand, honestly, to have conversations to introduce what we call Vanta Verified. But a continuous standard, right? So something that is not, “Oh, Vanta checked three months ago. And so it's probably good.” But it's like Vanta checked three minutes ago. And here's the real time dashboard. So it's what we're moving toward, and that's we tried to actually do that in the very early days. We tried to just walk around and give people Vanta dashboards. And mostly what we got back from startups was, “This is cool, but no one wants by Vanta dashboard.” They want me to have a SOC 2. So can you help with that? And so the whole kind of company premise is like, “Yes, we will help you with a SOC

2. But we do not see ourselves as a SOC 2 two company. We see ourselves as a company that is using SOC 2 to build the credibility and brand and capacity to actually have a continuous verification of software security. So everything we do is oriented around that.

[00:42:18] JM: So in the long run, you see yourself more as a security company rather than a compliance company.

[00:42:24] CC: We do, yes. Yeah. Again, compliance is like the purchase trigger gets people to care – Or to not really care. People care, but it gets the stonework prioritized, right? Because walking around in the early days, we'd walk up to CTOs at startups and be like, “How do you feel about your company's security?” And they'd be like, “Good in some ways. Terrible in others.” We’re like, “Cool. Can we help you? Like how can we help you make it better?” And they would say, “Well, step one, I have 20 other things on my list around unlocking new business, growing customers,” da-da-da. Then I can run around and worry about security. And so again, the insight was can you use one of the things that helped someone grow their business, compliance certifications, to help them prioritize some of the security work that they probably want to do, know they need to do? Just hard to prioritize on a fast growing startup.

[00:43:14] JM: When you're coming into a really big market, it often helps to have a really differentiated entry point. And you have a differentiated entry point. So you're entering – In the long term time horizon, you're entering a security market from a compliance standpoint. How does that impact where you guide the company?

[00:43:39] CC: So a few things. So one, our point of view on compliance is, and sometimes a little bit of a push pull with some of our audit partners, but like fulfill our vision. It needs to be rooted in engineering best practices, right? And so when we think about what are we recommending to a company? Like we will recommend code review, but that is because it is often a good engineering practice. We will generally not recommend keeping the fire department phone number on file, right? Like there's just something, you pick your old antiquated compliance thing, right? So there's a lot of like orientation around what are, again, what are the software engineering best practices in 2021? I think even there's a push pull with that, right? Because some of the audit partners we work with are more up to date with software engineering in 2021 than others, right? Like some containers are still like a totally for it, I don't

know. The thing you get and put your food in, right? And so striking that balance with them, right? There's some amount of education and some amount of here's what this thing is, here's why you only need to check one of them. You don't need to check all 40,000 of them, right? Things like that mean there's a lot of education around software engineering that we end up doing.

[00:44:51] JM: So you say you have 80 people at this point, and remind me, is there a heavy manual component to an engaged with a customer? Is there a lot of kind of customer success or consulting style work in the product strategy today?

[00:45:09] CC: So we do have a bit. I very much do not want to charge for any of it. Because, philosophically, I think of the bit of fat that we do as things we do as we continue to build out the product. And so I do not want us to get used to consulting revenue or professional services revenue or anything like that. But I think one of the other parts I've sort of mentioned this a few times is we do have customer success, right? And customer success team being sort of twofold product-focused, right? Product success. How do we get you set up understanding what the product is going on that front. And positioning CSM's truly as sort of security and compliance advisors. So able to sit with the startup and be like, "Hey, where are you selling? Who are you selling to? What are people asking you for?" Getting questionnaires, right? And sort of being able to guide them there, which again pushes on the education piece, because we need CSM's to be able to understand this stuff for a technical audience. I think the other part is we're not an audit firm. We work with auditors. And some of those auditors – Those auditor still operate service as businesses. And so they do a bunch of what I think a software person would look at and say services work they do because we share a customer relationship in a lot of cases.

[00:46:23] JM: Cool. So as you're going from this, the customer success model, where customer Success is on the critical path, to a vision where which would presumably be more automated, more software-focused, what's your hiring strategy or headcount allocation strategy between those kind of two divisions of the business?

[00:46:46] CC: Between like success and engineering say?

[00:46:48] JM: Yeah.

[00:46:49] CC: I mean, overall, like expect engineering to be a much, much larger portion of the company today for all the reasons that everyone knows. It's generally easier to make customer success hires and engineering hires, right? So in the past, we have been like, “Okay, we're going to do something manually. It's going to take more people. We're going to know it's manual. We are going to write down what we're doing so that we can turn it into code.” But I guess, in that sense, in the shorter term, having customer success prototype, product initiatives, right? Because, again, when it's like a process in a Google Doc and you have people running it, you can change and iterate on the fly and figure out, “Oh, this Oh, this is how onboarding actually works.” When you do things in this order people understand them, whatever it is. Here's how to actually explain how to choose an auditor and which one to work with. And then you can hand that to engineering and say, “Okay, here's what we think the order, right? And we still want to maintain some flexibility and iterate and da-da-da-da.” But we actually have a stronger point of view on how we want this product experience to be. And so in the longer – And then just in the longer term, like Vanta is fundamentally a technology company. And so joking, but not, I mean, everything is prioritization. But I do think we can solve the vast majority of our problems with software. It is just how do you prioritize what to build and when question.

[00:48:06] JM: Can you tell me about the technology decisions around the company? What are some SaaS providers or infrastructure platforms that have impressed you? What are some engineering decisions that the company has made? Build versus buy? Things like that?

[00:48:20] CC: Yeah. I mean, we really started building Vanta kind of late, true software, late 2017, right. And so we've bought a lot of. We never tried to roll our own metrics framework or anything like that. The way that sounds goofy to me today. But 10 years ago, people were totally doing. Let me think what do we do – I mean, built around AWS. So I think that was – A little bit of no one gets fired for buying AWS, right. And they will just have everything. I think the places where we probably ejected from AWS are more interesting, right? So we started using Cloudwatch metrics, and then realized Datadog existed and just like how much better it was, right? And so now kind of a logging and monitoring runs through Datadog, infrastructure, product, etc. There's a ton of instrumentation and alerting there. Early users of Terraform, like that was almost from day two. It was exceedingly frustrating to set up. And then once you have it set up, your life is a lot better. Seems like most folks, Terraform stories. Oh, we our primary

database to this day is Mongo. We used it initially, because it was easy to set up for a prototype, always intending to switch it out to a SQL database. And then you sort of never do those things if something takes off, right? You always have product features to build. And so maybe a year and a half ago, we migrated to Atlas versus just self-hosted Mongo. Just infinitely better. Having a team that's us maintaining it. Like that was –

[00:49:59] JM: By the way, even though – I will say even though Mongo is a sponsor of Software Engineering Daily, or at least a past sponsor. I'm not sure if they are right now. But I will say, despite endorsement, moving to Atlas has been really interesting for us. That tool alone has given me faith in MongoDB as a company.

[00:50:17] CC: Yeah. And I think even as some part of the package, we got like some number of like, solutions, consulting hours. We're like, "Oh, my God. I will never use this." Of course we did. And it was like, really helpful. Yeah, trusting them to run Mongo, not us.

[00:50:33] JM: Because so much so many startups are like, "Okay, I'll start on Mongo. And Mongo is the easiest thing to use. It's the JavaScript of databases. It's great. And it always hits some scalability problem. There's a whole meme around this, the MongoDB web scale thing." Everybody has their problems with MongoDB. It's kind of a hilarious meme in the industry.

[00:50:53] CC: Yeah. Talking about other things. I mean, the frontend has always been in React. I think they're probably uncontroversial in 2017 when we chose it, and it's super uncontroversial now. But like, you just get all of the nice things. The GraphQL layer I think we found is a little – Or is a very different paradigm for folks who we using it. But when you kind of use it correctly, not when you like basically build it. Like when you build a REST API on top of GraphQL, it's like just a worse REST API. But when you like actually use GraphQL in a graphy way, you can kind of get some neat things and neat properties.

[00:51:29] JM: Should companies use GraphQL from day one? Every company?

[00:51:33] CC: Oh, god! I don't know if I trust myself on this one. But like, probably. Yeah, but I think if you do just want to indoctrinate everyone in like the GraphQL way of thinking. Our first engineer, Robbie, wrote a document called the Zen of GraphQL that is mandatory reading for

every new engineering hire at Vanta. And I think that was actually really helpful. So one thing a company should definitely do, to your JavaScript point, is we started in JavaScript, and then in like – And I think it took us four weeks, which in retrospect, is insane. But it took us four weeks to switch to TypeScript. Every company should use TypeScript if you're going to use JavaScript. Every company should use something that is typed, just like the number of bugs we had just on the frontend. And then when we unified types across GraphQL, between frontend and backend, that just made life so much better. Can't imagine with dealing with that complexity would be like now. Every company should definitely do that.

[00:52:28] JM: Okay, great. So as we begin to wind down, just one final question about your background. So I look at your background, which back in 2010, more than a decade ago, you were at USV, which is one of the best early stage investment firms. You were there for about two and a half years. And then your career just basically looked – It looks like you were kind of wandering for a while. You were a professor. And then you started a labs company. And then you worked at Dropbox for a bit. And then you started a unicorn. So how do you get from wandering to starting a unicorn?

[00:53:04] CC: You know, no difficulty wandering, but I think that probably is what it looks like. I think it's actually too polite. So not to be Richard Hamming on it, but to be a little Richard Hamming, hopefully wandering with like some amount of purpose, right? And like I think his line was more colorful or something, like the drunk man will eventually stumble toward the light post. If you just set out looking for the light post, you're more likely to get to the light post. Not to say you're either drunk or super determined walker. But I was at USV. Really liked a lot of the job, but fundamentally wanted to be one of the entrepreneurs coming in and pitching. Couldn't code at the time. Wasn't technical. Didn't feel like I could start a software company. Even though lots of people who can't code start software companies all the time. I was just not someone who thought I could do that. So I took my bonus, lived off it two years, taught myself to code. Made a bunch of stuff. None of which anyone who helped me with this has ever heard of, but just learned how to make products. That eventually took me to Dropbox, which until I found my first real job, but the idea was in fact to start a software company. It just took some amount of stumbling toward the light post to get there.

[00:54:09] JM: Okay, that's great to hear. And I'm sure it will be encouraging to a lot of people. Thank you so much for coming on the show. It's been a real pleasure talking to you.

[00:54:17] CC: Thank you for having me.

[END]