Ep. 38 In a Town Full of Secrets . . . The Best Kept Secret

This is John Gilroy from the Federal tech podcast.

00:06
And this is Chris Townsend, Vice President of Public Sector at elastic.

00:10
Today we're gonna talk about elastic on, hit the music cloud. Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Well, last a con sounds like some kind of a superhero something, doesn't it? Chris?

00:28
It is a superhero event we haven't been able to do for the last few years because yeah, no lockdown. So we're very excited about Alaska con coming up on February 1.

00:39
I gotta get some kind of like audio effect. Oh, oh, no.

00:43
So when's it coming? When's the last con coming? When's it coming? Chris?

00:47
February 1 2023. John, we're gonna get our superhero customers and partners all together at at the event at the Marriott DC we're really looking forward to it. You got

00:57
to wear superhero costumes. But my daughter goes to these events where they're all these costumes and everything else, you know. So it's good. So I guess the question that everyone's thinking is elastic con. So what is elastic? What is elastic search? I think by now, many of my listeners have heard of this concept of Elastic Search. They have some basic idea what to do. But I wanted to get Chris in the studio today to explain to our audience, the value that elastic can bring to the federal government, how it can save money for the federal government, and maybe taller and more attend this event in February 1. But before we begin, give us a thumbnail sketch of your company, please, Christopher.

01:31

Well, first off, John, thank you so much for having me on. It's great to be speaking with you. Again. It's been a long time. I joined elastic about 90 days ago. So I'm brand new to the organization myself. And I'll tell you, John, and he hit the nail on the head. Elastic is one of the best kept secrets in technology. When elastic approached me about joining the organization, I had to do a lot of research myself on exactly what elastic did and elastic is a leader of it, they they have a started out as an open source company. It started out as an open source company founded back in 2012, by Shai Bannon, who lived in in Europe in his wife was a a culinary student, and he needed a way to search for recipes. So he built a search platform. And then that evolved into an open source development project, which evolved into Elastic Search the company back in 2015, they started acquiring a different capabilities and built the elastic stack. And from there, it's really taken off and we're approaching a billion dollar organization today. But in a nutshell, the platform sits at the intersection John of of data analytics and cybersecurity, right, the hottest, the two hottest spaces in technology and problems that our government customers are really struggling with how to solve and elastic underlies a lot of those capabilities across government and private sector and some of the largest name organizations out there. And both the private sector and government rely on elastics technology to do search to do data analytics on cross platform cloud platforms and on prem. They rely on elastic to secure their organizations to do full stack observability. So when I know we'll talk a lot more about it. But as you can see, I'm excited to be here. It's a great company, a great culture and some of the best people I've ever worked with.

03:19
Well, Chris, I've known you for a while and you're kind of a young puppy you don't remember back in 1971. Back in 1971. There's this guy named Marvin Gaye, DC native, by the way, and he released an album called what's going on? And Ivan did all this research on Elastic Search and cybersecurity and SCI M and soar and XDR. And it all boils down to what's going on. I mean, what you're can do is you can allow a federal agency to answer Marvin Gaye's questions, what's going on in my network and know in detail what's going on? Because of your ability to absorb so much information from so many different sources? Is that right?

03:58
Absolutely, John, and I love the way you put that. And I'll have to relay that to our marketing organization. Marvin Gaye spin on what we do, but you're right, it's, you know, it's it's hard to really define what elastic does, in just a context of a simple product category. Because you're spot on it, we have the ability to search and correlate data from so many different areas across multiple cloud environments across, you know, structured and unstructured on on prem. Again, and what this is the reason that it's so widely deployed in so many industries and relied on by so many organizations, because of the the platform is so malleable and so flexible. And because of the open source routes, it's in integrates with so many other tools and technologies. It's just a very flexible platform. And as as we try to use data to improve security or use data to better effect the mission of our agency or use data to provide an improved customer experience to the citizenry that's accessing government entities, elastic sits, you know, right at the nexus of that. And you're right, it allows our customers to understand what's going on in their environment where their data is how to organize their data, access their data. And there's just a ton of uses for that one of the most common uses that we see across the federal space is spaces is cybersecurity in organizing and accessing data to provide. We've also evolved into a full stack observability capability, where we can do things like application performance monitoring. So we hear a lot, you know, buzzwords, XDR, next generation sim, we deliver some of the most advanced capabilities in that area,

we acquired a company a few years ago called endgame that provides us visibility all the way down to an endpoint agent as well. Now,

05:55

we know Chris, there are people who may be listening to this, you know, a year from now or six, eight months from now. And one real nice thing we have is, is this podcast is gonna sit on the server, and people can access it and, and get more information about Elastic Search. And I was at your website today. And you've got this great report called the elastic 2022 Global Threat Report, we're talking exactly about what you just been doing in detail. And you can download this report, where the best place to go to find this report, what do you think?

06:25

Well, elastic.co, you can go to our website and download the report. You can also just go to Google and type in elastic Threat Report and pull it up. It was just released the other day, like you said, it's our first threat report that we've put out. And that was really, again, a response a response to demand from our customers and partners. We're doing so much now in the cybersecurity space across all of the public sector organizations. So the Department of Defense civilian, almost every civilian agency uses elastic in some capacity for cybersecurity, we're very broadly deployed across the DoD army and air force and increasingly Navy and and very broadly deployed it also in the intelligence community, as well as the state local areas. So not only our public sector, but our private sector customers were asking to, for us to publish report and talk about what we're seeing out in the environment, and what trends we're seeing what information we're seeing. And so we did we we published our first Threat Report, and we're pretty excited about it, well, you're

07:30

actually in a pretty good position, you're kind of like the middle linebacker, because you see all the threats coming from different directions. And because of that, you can have a detached opinion of what's going on out there. Because I see working with Google and AWS and Microsoft, and working with you kind of like a Swiss Army Knife worked with all these different companies. But the advantage is you can get to see different threats from different organizations, and you can present it in a way that's not going to be biased, it's going to be objective. And I think that's what's really important for these reports is that a federal agency can read this report, and then project where they're going to focus on next year, and it's probably not going to be on the distributed denial of service attacks, it's probably going to be something to do with fishing. But I think reports like yours will reinforce that.

08:12

In you, you're spot on, John has always, you know, it really comes from our open source roots and are and that's one of the reasons our customers are so passionate about the technology because, you know, we're an open source cause we're an open source capability, our customers, you know, trust us, and they've used this for a long time and built this into their, into their platforms. And you're right, because we are cross platform, because we run in Amazon and Microsoft and Google and we run on prem, we have broader visibility to a lot of the threats and a lot of the trends that are occurring today. And you know, it's it's funny, I've been in cybersecurity on and off since the late 90s. And you know, as it relates to cybersecurity threats, what's old is new again, right? It's, you know, credential access, and not using two factor authentication and not using strong passwords that are still creating a lot of the vulnerabilities in the Cloud Platform. You know, adversaries or bad actors are still trying to repackage old tools, it's very time intensive and, and expensive to create a true zero day new tools like building a new piece of software. So, you know, we're seeing a lot of trends around obfuscation and repackaging of old tools using Trojans and other devices to be able to bypass the detection of of endpoints and other security tools that exist today. But you know, which which has been happening, right forever, right, in terms of in terms of the cybersecurity threats we're seeing, but we are also seeing some new and industry interesting trends around increased focus on on Linux endpoints. So 39% of the malware we're seeing today is focused on Linux and you know, used to be the preponderance of of your attacks were targeted toward Microsoft and they still are 54% is focused on Microsoft but Linux F boys a 39% is high and you know, that's Again, one of the reasons that we moved into that endpoint space with that, that acquisition of endgame because that that is a that runs on a Linux platform as well. So we can protect Linux, Linux access points. But that's definitely a trend we're seeing, which you would expect as we increasingly move to cloud. But the Threat Report is great. It's very comprehensive, it does have some unique trends in it. And of course, it does talk a lot about, you know, some of the old threats that continue to be repurposed, but remain effective.

10:27
Well, you know, he said, endpoint, I'm taking notes here. And I recently did an interview with a guy named Dr. Tim Robinson. And he's pretty vendor neutral. And he talked about securing things on the edge. And you can listen to that episode 37, if you want. And this is a guy who was in the Marine Corps, and he earned a PhD in computer science. He said, When he started off, he had a rifle and a router, spices love that interview. And he would be a good guy talking about edge points. And maybe he would recommend using elastic depending on the specific application. He's very careful about what applications he would use for a warfighter, and what do you use inside an office? And so I think that's part of elastic is being able to be that flexible to know where to adapt for three letter agency or for more US civilian facing agencies that right?

11:12
Oh, again, John, you're spot on, you really do your research? Well, absolutely. One of the one of the great things about the elastic platform is it is so flexible, depending on the environment in which you want to use it. So if you've got an environment where you've got, you know, very well trained security operators, that are able to ingest in use the information to go after bad actors in real time, that's a different capability than maybe you want in a tactical environment that has to be effective. But but but very basic, and often in a detached environment. So that's one of the great things about elastic, because we're not relying upon connectivity to be able to do policy enforcement at the edge, right, our endpoint can work in a detached environment where a lot of the endpoints today are focused on the cloud and fight attachment.

12:01
Yes, yes, yes. Yes, keep talking, keep talking. Because the military guys out there saying keep talking, keep talking, keep talking, because they may be a middle of nowhere have have nothing. I mean, disconnected, and maybe a satellite link, maybe not maybe nothing. And so you have to have that flexibility that some systems may suggest or may put on their printed brochure, but may not really have a

12:25

that's that your again, John, you're exactly right. And look, the cloud security tools that are out there today that can pull down information in real time with the latest threats and dynamically update their platforms are great, and they are really helping, you know, the the good organizations out there stay ahead of the bad actors. However, that doesn't apply to every environment, there are still a lot of disconnected environments that just do not have that cloud access for a number of reasons. If it's a tactical deployment out in the Middle East someplace, or, you know, it's it's in a secured environment, in the intelligence community, it's air gap, you can't always have that cloud connectivity. So it's important to be able to still drive that security and provide that that level of security in an air gap, disconnected environment. And elastic allows you to be able to do that. You mentioned

13:11
Linux. And my first image was I was at a trade show once interviewing people from the floor. And this guy showed up with this penguin. And I interviewed him about Linux and back and forth. And, and I never thought of Linux as an attack vector. But I always associate open source software with Linux. And I've heard the term mentioned in regards to Elastic of open security. So open security, maybe can define that for our audience, please.

13:37
Yeah, you know, open security sounds counterintuitive, right? You think security should be in a black box and very secretive. But at the end of the day, more transparency and security tools and developing security capabilities and sharing capabilities around security is is really important and makes the fact of the more collaboration that we can drive between public and private sector and really develop those open capabilities and those open tools, the more effective they are against the bad actors. You know, when you start to develop things in a black box, it's easy to miss something where you inadvertently create a vulnerability and a tool set that allows the bad actors to exploit that so open security is is a great concept and one obviously that'll last it's very supportive supportive of whether again, whether open source routes,

14:26
I gotta fall back on my roots, my radio roots. So for information elastic, E L, A S T IC dot C O, lots of information there. You can download the current report that's pretty easy. So we've got open source with open security and I want to toss out a four letter word and the word is sore SAR I had on the edge there didn't I just saw soar fitness conversation. I love the acronym who where does it fit in the conversation?

14:53
Yeah, security, orchestration, automation and response in the holy grill and security has always been John Again, back when I started the industry back in the late 90s, was to get the tools to work together in an automated fashion. So hey, if you detect something at the edge, you detect something in the network, you detect something at the endpoint, the tools could correlate those events in real time and take action against the bad actor trying to exploit your environment. Now, there's, there's some reasons that we haven't fully automated the security environments, because false positives, you can end up you know, doing more harm than good in some cases, but sore platforms are, are increasingly commonplace in in your security, operating environments in your socks. And elastic can feed those sores, all that data that we talked about earlier, that we

can go out and collect the cloth across multiple platforms and aggregate that data, we can feed those sore platforms and give them the data, they need to be able to take those automated responses against those bad actors in real time. And, again, because of our open source routes, were very easy to integrate with most software tools out there. So again, you know, we've got partnerships with just about all of the software vendors out there and do a lot in the background with a sock environments to feed that feed those source with our data.

16:15
Yeah, I know people from Google, AWS, Microsoft, and you're probably played both all those different companies together. I have to ask this question. I don't want you to name names. Remember, the Seinfeld episodes are going to name names. I don't want you to name names. But I want you to give it perspective. For listeners. You know what? I didn't hit the record button. Ah. You got another half hour?

16:40
Oh, we didn't record any

16:41
I didn't hit record. Now it's recording. It's recording? No, no, it's recording. It's recording. Yeah, I minimize the screen. Oh,

16:49
you're messing with me, John. But yeah, I would of course, it would have

16:53
been? No, I was I was minimizing the screen to look for something. We'll have to edit this out. Okay. Where's my thought process? It was okay. Here we go. Okay, now, Christopher, I don't want you to name names. But I want you to take and talk about challenges that other people have had in accomplishing this task, you know, in other words, how do people fail doing this coordination? It must be challenging to do with all these different forms coming in. So So what's the biggest challenge people have in doing this kind of coordination?

17:22
Yeah, it's a great question. So, again, if you look at it just from the SOAR perspective, it's the challenges always around the false positives and integration of the tool sets. And the commonality is the language and the way the tools communicate. And a lot of companies out there have tried to build brokers that allow you to integrate or orchestrate information from different tool sets to be able to take action, but it's really the ability to collect that data, keep those you know, keep that communication platform up to date, so that you can ingest information from multiple tool sets in a common way to be able to take a common action against the threat. And that's, that's still evolving, in terms of the data collection, really, we're elastic thrives and again, collecting and aggregating and searching that data and doing it very, very quickly. You know, we do it in a very efficient manner that allows you to tear your data so that we allow you to store data that you may not want to need to access on a regular basis, we allow you to do it in a way that's less expensive, but you can still get to it relatively quickly. And you can imagine as the datasets continue to grow, and they're growing exponentially.

The cost of indexing and maintaining those data stores is really expensive and elastic, does it away does it in a way that's extremely efficient. We'll we don't force you to replicate the data, we have this capability called cross cluster search, which allows the data to stay in the where it resides. So you don't have to replicate it back into our platform. And it's extremely efficient, extremely effective, and and much less expensive. So, you know, I would say that's one of the biggest challenges in terms of handling data is, is the cost associated with handling data and forcing our customers to replicate that data which which we don't do.

19:16
I want to go back to Microsoft. We mentioned them earlier, kind of in passing. Last week, I was at a coffee shop in Ashburn, I was gonna walk into my car, and I someone got up and as a friend of mine, who worked for a very, very large Microsoft partner, and Microsoft kind of interesting the last Microsoft event I went to Red Hat was a speaker. And so I think that you folks work with Red Hat and I imagine with Microsoft as well. So when it comes to Microsoft was your any stories to tell our audience about how you work with them?

19:45
Yeah, absolutely. We have a great partnership with Red Hat as well and you know, their OpenShift environment with new most popular this year they It helps organizations more easily search, observe and protect their applications, data and infrastructure. Hey, Chris.

20:05
We just sent we dropped some packets there. Let's all start with the question again. Okay, okay. Now, Christopher, last week, I was having coffee and Ashburn, as I was walking to my car, I literally bumped into a friend of mine, who is a vice president of a very large Microsoft partner. And so my question to you is, I know you work with folks at AWS and Google, you also work with Microsoft, any success stories for them?

20:30
Yeah, we have a great partnership with Microsoft. In fact, earlier this year, we just found just signed a new multi year agreement with Microsoft Azure, that helps organizations more easily search, observe and protect their applications, data and infrastructure using elastic cloud on the Azure portal, the Azure platform. And you know, this increases joint investments across technology integrations, and the go to market and CO selling activities that we have with Microsoft and last cloud. So we have a very close partnership with Microsoft, as we do with with Amazon and Google as well.

21:03
Well, now it's time to get up close and personal many years ago, they those shows, but the Olympics up close and personal. So you say you've just been Elastic Search for a little bit here. So what surprised you about Elastic Search? What what did you not expect?

21:16
I John, I was blown away by how widely deployed elastic is in both the private and the public sector. I mean, the largest, you know, customers, the household names, the industries, the private sector, interested

customers out there are all using elastic, all the public sector organizations are using elastic, we're so widely deployed, and DOD and civilian, the intelligence community highly realized that elastic, I was I was just shocked about

21:45
I've got to use your lead in from a few minutes back, you know, in a town full of secrets, the best kept secret in town is Elastic Search, isn't it?

21:53
It is it is your right, John. And one of the other things that I was really just blown away with was elastic was was the culture here and the people, it's a phenomenal organization, great culture, one of the best I've ever been a part of, and working with some of the best people in the industry. So it's, it's, it's, it's been, it's been great, you know, 90 days in, but just really blown away by by the passion that our customers have for the technology, our passion our partners have for the technology and how widely deployed the technology is across both public and private sector.

22:24
I think that's really the summary. The headline for this interview is that I've known lasting for many years, and every time I speak to people elastic, I'm just amazed at the wide variety of organizations they work with. I mean, they're in so many different agencies. And by the way, in the commercial world, in such a wide variety of commercial areas, too. It's just it's, it's sometimes it's hard to describe what elastic can do, because it's so flexible and malleable. It's I see it in banks, I see it in financial, the Treasury, I see it all through the DOD. So it's a one hat, it's easy to describe, it's difficult to describe So isn't it?

22:57
It is it is because it's truly a platform, right? Everybody wants to be a platform, every talks, everyone talks about being a platform, hey, we're the platform for this, we're the platform for that. But if you look at what we do at elastic, it is truly a data platform that can, as you said, it's very malleable. And there's a lot you can do with it. And our customers continue to find new ways to use elastic to organize and search their data. And again, you know, cybersecurity is a big focus. Now, you know, application performance monitoring observability. And then, of course, it's our customers are using data more and more and more to affect their mission. We sit right at the nexus of that. So it's just an exciting time to beat elastic.

23:37
So Chris, I'm gonna give you the final word here. So where do you think Elastic Search is going to soar in the next few years?

23:44
Yeah. Well, like I said, John, we're just crossing the billion dollar threshold. And I this is just the beginning. We're growing like crazy. We've got a wonderful organization, we got lots of lots of open open positions. So if anybody's looking, please come to the website, check our open positions, we're hiring and we're growing like

crazy. You know, I think we're, you know, in the next couple of years, we want to be a $2 billion company, but I think we're gonna blow past that and, you know, see five $10 billion in the not too distant future as our customers increasingly rely on data for all sorts of of mission applications. Again, we're just really at the nexus of of, of many of those efforts. Great.

24:27
Well, unfortunately, we're running out of time. I'd like to thank my guests. Christopher Townsend, Vice President at elastic Thank you, Chris.

24:33
You're welcome, John and don't forget elastic on February 1 2023.