FEDERAL TECH PODCAST

Episode #22 Tony D’Angelo Lookout Federal Endpoint Security

SUMMARY KEYWORDS
devices, threat, apps, agencies, lookout, mobile device, ransomware, trust, tony, data, attacks, mandates, phishing attacks, cloud, mobile, endpoint, effectively, government, pegasus, perimeter

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Our guest today is Tony DeAngelo. He's the Vice President for US public sector had a company called lookout don't have to spell that Tony do i Everyone should know look out by now.

00:59
Absolutely Good to be with you today, John, thanks for having me.

01:02
We are going to do a little Hocus Pocus, who's got the focus? We're gonna talk about COVID and transition to mobile and mobile attacks. And then we may throw in a little zero trust in there. And the reason I contacted lookout was because after all these hundreds and hundreds of interviews, I've done it I've never given an opportunity to someone like Tony to tell his story to the federal audience. And so Tony, I want you to do is know my listeners Latimer guppies, and they scratch their head, they see this company and that company and and it's what's in it for me. I mean, that's all about so if I can show them Look, look out as this, this this, this is how they can save you money. This is how they can reduce headaches. Really, that's what they want. I mean, you know, Tony might be a nice guy. But if you ain't saving me money, well hit the bricks, buddy. So give us a quick thumbnail on out on lookout and your background, please.

01:48
Yeah, you bet. So thanks again for having me. I've been in the in the industry over 30 years now all of it in the Washington DC area and working with our government clients. About to look out about four years now look out is is a company that's got its roots in mobile security, we've been we've been around a little over 12 years now. And that, that that routing in mobile security is key because as, as we've seen over the over the past couple of years, just the demand for mobile devices and access to government assets continues to increase dramatically. And, and with the with the pandemic and the and the drive to telework, and frankly, COVID and the pandemic have increased dramatically telework and work from home folks, those assets in the ad, the demand to access those government assets via mobile devices only continues to increase. Therefore, with that being said, the the threat vector and the attack service on a mobile device also increases and and we see that on a daily basis with all of the threats that we discover. So in addition to that, look out has expanded into the cloud security realm as well. And we fit very well into what you mentioned a moment ago, but zero trust would

fit into the zero trust elements that the White House and OMB have have dictated and very well in it. So effectively, you can think of lookout as protection from the mobile endpoint up to and to occlude all of your data in the cloud.

03:28

Now, there's a podcast in town here, the Husky has and it's called Feds at the edge. That's where I talk I should duck the title of the episode Feds at the edge talking about today. Now, the elephant there, of course, is COVID. You know, when you think of before COVID, there was certain agencies that were I think the Patent Trademark folks were remotely accessing, but vast majority weren't all of a sudden, we have this big ramp up, and a lot of lessons to be learned from that ramp up. And the folks over at Verizon, kind of a third party information play the they do this annual study that Deborah DVIR and talks about this and that, and I was reading it before this interview, and I'm telling you know, it's it's, you know, you're about to hear about supply chain and supply chain problems. And, and each federal agency has a supply chain because they don't manufacture anything software, they have to go through something. And so what the Verizon report shows is that 62% of breaches were caused by partners and partnerships. So, Tony, even if a federal agency is listening to you and doing all the checkbox things, so what I mean, it's a whole lot more than just to focus in an agency, isn't it?

04:29

It is, it really is. And fortunately, there are technologies that can can address those things today, even even though with the with with cloud security solutions, we can we can protect the data wherever the data goes. And I think that's an important element that these agencies need to consider with their partners because you're not going to be able to control everybody else's network and the security on everybody else's devices or desktops. So there is going to be that element of kind of weaving in this notion. have continuous conditional access, not trusting the user not trusting the device, not trusting the network that it comes from. And, and effectively using things like behavior analytics to, to identify where these threats might occur. And again, following that data, those documents wherever they go, and wherever they come from, that's going to be an important item, like watermarking. And redacting and things like that.

05:26

Look, out.com, I went through this morning. So white paper, just specifically for my gov is for the Federal audience. And it talks about a case study where a certain company used lookout and had all kinds of good success with it. And at the at the the bottom at the footnote, kind of at the end of it, it says that our platform uses AI to analyze data from 200 million devices and 100 million apps will do the math on that. I mean, how can even keep track of that many apps and devices and the complexity is beyond understanding.

05:59

It is it's exciting in the same way, right. And you think of why we've been so successful in in mobile security is the efficacy of the solution. And with 200 million devices running lookout, you think of it as almost like a crowdsourcing method, right? Where so all of the web searches all of the clicks, all of the downloads, we're learning from all of those devices continuously. So just gets us closer to being able to predict all those zero day

attacks. And, and the 100 million downloads of apps. And we scan every app on every app store, whether it's iOS or Google Play, and or the Apple App Store or Google Play. And then all of the other third party app stores as well. And we have a library of all of those those past apps, those past versions of those apps that are no longer on those app stores. If you think about any, any company or organization that would want to get into this business today, they just don't have the history of all of that all of that data that we've been collecting over the last dozen years or so.

07:05
Yeah, there's no software technique, they'll take some code, and then compare it and have software, they'll convert and find the changes. One of the problems is no software technique, but it works here. You know, and, in fact, what some people say about you, but your company is that you can identify zero day attacks in the application. So this is almost like, no one, someone's going to try to steal your car you put in the garage or something. So this anticipation that that's a very powerful tool to have.

07:31
It is indeed and again, it comes from comes from all those devices, all the machine learning from all the clicks, and and all of the threats that we've identified in the past, because a lot of those a lot of threats from the attackers are either reused or slightly tweaked and used again, and a lot of them have the same, the same signature. So we can we can see those jailbroken or rooted devices, we can see the behavior on the phone that gives us cause for concern.

08:00
And public speaking, they say it's easier to change the audience than the talk. So they've been done that a lot. Gotta go back to the surprising thing of just fascinated me. They talked about the likelihood of an attack the likelihood of a breach, they said, Look four times as likely from an external source and an internal source for a breach. That's someone on the phone, isn't it? I mean, this could be your contractor. It could be it's, it's just it sets you up for telling the story.

08:26
Yeah, it absolutely does. And further, you know, further reinforces the need, if you're talking about specifically just mobile devices is to is to provide this just to put them mobile security solution on a on a on a device, tablet, and phone. And it's critically important. I mean, the internet traffic today. I mean, it's depending on what statistic you read. The amount of web traffic that comes as originated from a mobile device is north of 50%. And a lot of statistics now put it in the in the mid 60s, I've seen statistics as high as 70%. I mean, that is tremendous. And then and then it goes back to again to telework, right. And even with the pandemic waiting now we also have the return to travel. So that means free airport Wi Fi coffee shop Wi Fi, hotel Wi Fi, you're out in the wild with your mobile device and their attacks are plentiful. I mean, even during the pandemic, I noticed just a massive uptick in in tech space phishing attacks, you know, from large, commercial carriers telling me to click here to check the status of my package. While I didn't. I didn't I didn't order anything. So I know that those were phishing attacks, and I see those. They've increased 50 We see 50 to 75%, depending on the agency now in terms of mobile phishing attacks for devices that we protect.

09:52
I'm a big fan of Mission Impossible movies and he always says technology is amazing. And that's amazing. I don't know what to believe what not to believe. When I started reading about Pegasus and about Trident, it dawned on me that perhaps there are agencies in the federal government that have to be careful about what is allowed on their mobile devices. And so I gotta beat around the bush here, but But you do a whole lot more than just prevent malicious attacks. A lot of prevention here.

10:21
Yeah, exactly. A Pegasus is very interesting and very scary. I mean, that was developed back in 2011, by the NSO group. And that is a spyware that, with certain apps, were able to be loaded onto a device with zero click, meaning I could send it to you through the airwaves, without you even answering a call or clicking on a link, it would be loaded on your device. And with that, I could I could see your GPS locations, I could read your text, I could see your photos, email, effectively a keylogger. And I can see your username and password. So there are to your point about restricting what is on a mobile device. I'm sure agencies vary and will certainly do that the type of secure data or intellectual property that can reside on the device, a lot of these phishing attacks and a lot of these, these, these threats, like Pegasus are used for credential harvesting. So they don't necessarily want what's on the device, because there may not be much on that device. But they'll take your credentials, and use that to access other parts of the network. And then they can go horizontal through the network that that is typically the greatest attack. factor with a mobile device, frankly, is the credential harvesting.

11:39
So let's expand on this. So if the folks at NIST tell us that the five pillars of zero trust, the first pillar is identity, and your identity can't be compromised through you telling me identity can be compromised through my phone, without my knowing it could be

11:56
absolutely 100%. So select to spend

11:58
more on zero trust. So you say have an initiative and to help our good agencies with zero trust as well. Is that correct?

12:05
That is correct. Yes. And, and mobile, mobile, certainly part of that as well. We've even seen, one of the OMB mandates focus on EDR, which is endpoint detection response. And that's not just for, for the for desktop endpoints, but mobile endpoints as well. And so that's a key tactic for being able to see the activity within the devices or endpoints on your own network and do some proactive threat hunting and analytics based on that.

12:37

Threat hunting boy, that'd be a good Mission Impossible title, wouldn't it that threat Hunter, tell us about what about your the lookout threat lab and what they do?

12:47

Yeah, sure. So we've got a group of threat researchers, they've been, they've been with us for a long time to large organization, and they spend their days searching the globe for threats, they look at the threat data that we collect on the devices, they look at how each of these threats morphs from one thing to the next. And they use a lot of this AI and machine learning and analytics to try to prevent the next attack. And a lot of what we do is, is we see the behavior of the device. And again, whenever we we see, of course, there's there's there's investigating links, you know, we've got blacklist blacklist and whitelist of links, but it's an investigating all of these, these phishing potential phishing links. It's, it's a, the the apps, the threats that are based on the apps and then that could be malware inside the app, or it could even be something somewhat benign, which is, what is the behavior of that of that application. And you might download an app that doesn't necessarily load malware on your on your mobile device, but it could be exfiltrating, all of your contact lists and sending them to China, right? So so we look at that level of of stuff as well. Because when you click on a on an end user license agreement, and I mean, how many of us actually read those things. You click Accept on the on the EULA bait, we've even found baked in those EULAs times where the behavior of that app now it's telling you what they're doing. But it's telling you that it's going to send all your data to China. Now, you may or may not want that, right? We probably don't. But we're looking at all those things. So just the the the malware but the behavior of the apps as well. And then you look at the this, this kind of notion of all these phishing attacks and what they're doing and how the device is behaving based on the the user intervention and all that gets baked into our threat intel, we we can share that with end users. They can use their own their own data from their own networks to do endpoint detection and response, as I mentioned earlier, and try to get ahead and really the whole basis of all of this threat intel. And what we can share with our clients is to get to move from playing defense, with cyber attacks to playing offense to try to get ahead of it.

15:11

I'm trying to come up with the analogy here, some kind of illustration. Last summer, my wife and I drove to Ohio to visit friends on a farm. And there was an app that my wife was using, and it said, something in the road ahead. And it was a bicycle. And so I swerved out of his bicycle, that would have been a bad day on the Pennsylvania Turnpike. And so the reason they derive that is by crowdsourcing information. And so there is a threat lab a compendium of information, saying, Hey, Tony, there's a bike in the road there, be careful. And so we can probably apply that to a lot. Look, I mean, if you have that many millions of devices, and have that strong a library of of apps, then then what you're providing is almost, I don't want to say the word, but maybe it's continuous information on threats out there. It's almost continuously monitoring the threat landscape and, and updating it regularly, how else can you do it?

16:06

It's a living breathing thing. So our Threat Graph has, you know, a couple of billion data points on it via via the manner in which you just described, right, which is somebody sees something could be a coffee shop Wi Fi, where, you know, it's there's, there's a fake network that we identify that it could be, you know, a malicious app, it could be a phishing link, all of these things, continue to provide intelligence into the system. Now that,

you know, humans per se, don't see anything that we're doing on individual devices. Now, they'll they'll see threats out into the wild, right, that we're investigating, but users should know, you know, consumers and, you know, public sector, private sector like that the the system is protecting the devices and the AI and machine learning is, is seeing what is occurring. But you know, there are not human just like Pegasus or no humans that are looking at personal information and personal data and things like that.

17:06
When I think of zero trust and cyberattacks, I think of ransomware. I have a friend who owns a small company in Virginia, and I said, Hey, boy, do anything. Make secure backups, make sure they're immutable. You can backup if you're attacked. And so I think there's one strategy there of having good backups. But I think your strategy more is there's more prevention than then trying to recover from the backups, because inevitably, backups are going to be problematic. I would think so. So what lookout, that's the word look out for what's coming.

17:36
Look at right defensively put the emphasis on the word. Yeah.

17:40
Yeah, exactly. From Navaho, behind from lookout ransomware is coming. Let's start with somebody. Yeah, that would be a good way to introduce yourself at a trade show shouting there. So what about federal agencies? Do you know of any admin attacked by ransomware?

17:54
Um, yeah, you know, they they, yes, we do. State and federal, and some of them are, some of them have made it known that these have occurred and others have not. I mean, even at the state and local level, within the Washington area, we've, we've seen a few over the last couple of years. They're there, they're quite prevalent, and you see him in school districts, they're particularly vulnerable K through 12. Schools, they're, you know, they, they oftentimes don't have the budgets, or the bandwidth of, you know, the size of IT organizations to, to build the proper reinforcements, so they can be victim to that as well. Off unfortunately, even though ransomware is is incredibly expensive. We see a lot of these agencies and organizations paying it. And because the alternative is, you know, you could spend two or 3x that we're either having someone come in or with your own staff trying to restore your data.

18:56
Well, if you're a small business, and you employ 30 people, you can write the check and move on. But I said, No, no, no, you're setting yourself up to get hit again, just down the road

19:07
to go to the federal government self insurers, but we do see state and local agencies that will buy ransomware insurance, which is interesting. And we're also now seeing insurance companies dictate to the policyholder that they need to have a certain level of security stack in place because what they're because a lot of these

organizations have said it's cheaper to buy ransomware insurance and they buy the insurance but yet they don't you know, beef up their their their forces on the back end. So effectively, the insurance company has high risk and they're left holding the bag so I think the the underwriters have figured this out and maybe they began to to just just just like you know, when you buy a personal life insurance policy, you have to get a physical and get some blood work done. Check your cholesterol check your blood pressure insurance companies figured out they need to do the same kind of thing with with the policyholders because they may, there may be a level of either recklessness or, or low, low integrity defenses that will cause them to have to pay out. And they don't want to pay out. Very interesting as this whole world of ransomware evolves. There's so many pieces that it touches, and again, to include these insurance companies. Well, Tony,

20:26
you've been around for three decades, you've seen a lot of good stuff and bad stuff, got the T shirts got the scars. So let's look 30 years the future. Now let's look 340 years in the future. So where do you think this all heading zero trust is going to be embraced? Do you think they're going to back off on it? Do you think there's going to be a threat that's going to so I think there's going to have to be some kind of an incident that's really going to put a fire under people. But I want to hear what you say. Yeah,

20:51
that's a good question. I think if I if I look at what the what the government has, with the federal government at the federal level has mandated around zero trust, I applaud it. And we've we've seen architecture documents, with the civilian agencies as well as DOD, they're just slightly different. But they largely overlap. One, I think, has five pillars, one of the seven pillars, but But largely, it's around the same type of thing. It's continuous conditional access, it's trust, no user, trust, no device, trust no network, and do this on an ongoing basis. Again, the C and NCCA continuous conditional access. One of the challenges with you know, with the Fed has always been the scale. And, and, and a lot of these mandates often come out like this one did without necessarily having budget attached. So there's a mandate with a series of directives. And but then the government put in place, the ability to begin to fund this into their into their two year budget cycles in FY 24. So I think I would say we're probably seeing right now we're probably seeing kind of maybe where you know, the 8020 rule, or more like 8010 10, I think 80% of the agencies have spent the last 12 months or so since the mandates rolled out, trying to understand what zero trust is trying to try and do understand where they are in each individual agency, how prepared they are, where some of the holes are, the gaps are, and then beginning to look at the vendor community to see what different types of technologies are out there that are being offered. And then the thing I think that you've got, you know, 10%, that are leaning in pretty hard, and already probably had a pretty good idea of where this was going, had already moved a lot of data to the cloud and already begun to secure that data in the cloud. And then you probably have 10%, that are probably a little bit behind, I'm sure they're going to catch up. But there might be some some of the either smaller agencies or ones that hadn't moved a lot of data to the cloud yet, and therefore hadn't had the need to secure a lot of data in the cloud. But But I think, you know, the, the message is clear is that virtually every agency has or will move things to the cloud. Most of the large software vendors are no longer even allowing on prem applications of their of their offerings. So that certainly part and parcel forces people to the cloud for at least commercial applications. There's a whole series of legacy apps and government data centers that need to be thought through and how, how we secure those because they're no longer perimeter based defenses. So if you were

sitting in a government building, using a legacy app, and a data center that was physically in your building, and you had a a cyber defense that was effectively a perimeter around that all was relatively well. But now with telework, remote data centers, there's a lot of reason why all of that is effectively considered in the cloud as well, and things that need to be secured. And then just as general web browsing and out in the wild, as as an end users, all those kind of three areas need to be secured and secured effectively. And in that you're going to see that as well as endpoint protection. And some of the proactive threat hunting as part of all these zero trust initiatives, but they'll get it they'll get it done. And then they always do. It takes a while. But just the conversations we're having and and the opportunity that we have to be trusted adviser to a lot of important government clients is we're, it's refreshing to see how well they do understand this technology, and how many of them do have a plan in place to execute on.

24:27

Now when you said the word perimeter, I flashed on an article I read this morning from a well known pundit. And he said, the app is a new perimeter. Well, if that's the case, and Tony is positioned pretty well, because you have such a deep knowledge of the app, but that's interesting illustration of, you know, the, the modes and the walls and the but everything's inside and really the apps Jeff and the data is probably part of that discussion as well. Well, unfortunately here, Tony, we're running out of time. You've been listening to the federal tech podcast with John Gilroy. Our guest today. Tony DeAngelo. Vice President US public sector at Lookout