Jason Lopez:
This is the Tech Barometer podcast from the forecast, I'm Jason Lopez. About 15 years ago, working on an NPR story, I talked with security analyst Bruce Schneier. It was after the dot com bubble had burst. And for many users a seemingly new thing was happening: malware. It was escalating, but my assumption was the IT community would figure this out, to which Schneier said, “No, it's only going to get worse.” And today we're in the middle of a ransomware epidemic. We've seen utilities attacked and it raises the question: what about some of the most sensitive data out there, like military intelligence and defense? I talked with Nandish Mattikalli, chief engineer for the intelligence solutions business within the security sector at BAE, a company that has the U.S. department of defense as a client, and started by asking about his special sense of responsibility when it comes to it and cloud security.

Nandish Mattikall:
Yeah, it is not just a sense of responsibility. It is a significant responsibility, especially when it comes to cloud computing and that responsibility is related to the type of mission, the type of customer, the type of programs that we support. The responsibility, not only to continue the mission, but also make sure that they're all secure. Cyber security is a major risk element to make sure that both the internal, as well as the external threats are addressed, litigated, controlled and continuously monitored. Definitely a significant part of our emphasis. And especially with the cloud, that is one of the major concerns for adoption of cloud computing. Whereas the sense of security our customers would have when they have on-prem data centers or infrastructure, that sense of urgency for cyber comes down a little bit, but it gets enhanced in a cloud environment. And rightfully so.

Jason Lopez:
What's an example of the kind of threats that you see at the level of national.

Nandish Mattikalli:
Yeah. I will just take the example that colonial pipeline hacking. The implication of hacking those kinds of networks, it can bring our infrastructure of our country to bare minimum, and it will have significant impact for not only operations of our, you know, financial networks or defense networks, but from the security perspective, it could be any applications that if you're, let's say, for example, you are in a hurricane zone, right? Hurricane Ida is hitting our coastline and somebody is trying to hack FEMA's application. And if that application are secure, we are putting our people in danger.

Jason Lopez:
Right. You know, national security, I guess when you step back is more than just military, but it's things like disaster response. But I want to back up and ask you a question about you for a moment. And you grew up in India where, you know, there's been a national focus on information technology, education. How did you get interested in IT?

Nandish Mattikalli:
Yeah. So, uh, I was always interested in building and we used to play on the side of where you are in the sand and we always build sandcastles. The idea was how tall can I build before it breaks? So as I was going to school in India, India was sending satellites into space. So that really piqued my interest. And as I was working towards my masters at IIT Bombay in India, we were in the very early stages of an information system to handle satellite data that we're getting from multiple sensors in space. So building things and see how they work and make things that are impossible using math and science, I think is a significant driver. Even today when a plane

flies in sky, I look at it and say, wow, it's just amazing. I'm fascinated by the engineering. And I want to build new capabilities.

Jason Lopez:
Well, that's really interesting. You know, here at the forecast, when we interview people, we like to, you know, focus on them as more than just an expert with a title, but kind of get to know what's sort of under the hood in terms of what they think, but let's go back to that. Let's go back to the question of it. Where does BAE show up in the stack?

Nandish Mattikalli:
Yeah, absolutely. That's a very good question. So the traditional cloud computing model, there is a platform as a service, software as a service and then application as a service and then data as a service. And now we are into the AIML as a service. And where BA was before cloud computing, we were in almost all the layers. I Mean infrastructure and the platform and applications. But with the cloud computing and, um, infrastructure becoming commodities and platforms are becoming commodities. So we are moving away from the infrastructure layer, definitely. And we are slowly away public platform layer, but mostly focus on the applications, the data and mission outcomes and AIML layer of that stack. At the same time, focusing on security across all the layers, right? And in some cases there are examples where the customer wants us to build out infrastructure. We do do the infrastructure layer for the customers as well, whether it is a data center or a facility build-out. And we work with partners such as Nutanixs and Dell and VMware and other partners to help with those as a lead system integrator for our customers. But, the emphasis has been to move up the stack and not to be in the infrastructure layer where those are becoming more of a commodity.

Jason Lopez:
So when you step back and you, and you look at IT, has security always been a part of what you do?

Nandish Mattikalli:
Yup. So the answer, your question is, yes. The reason I say that is because the security mindset and the business that we are in the customers that we support and the missions that we engage in are the national security intelligence and defense customers I mentioned to you. But what we are seeing is attacks are evolving, right? There are several incidents including that of Snowden. The insider threats are much more prevalent and more dangerous with the multi-cloud our attack surface has increased. And there's a interest from the nation states to disrupt our operations. So as our adversities that change the game, we are rapidly evolving as well.

Jason Lopez:
Well, what would happen if a defense project was compromised, what would occur there?

Nandish Mattikalli:
So a defense project can be at various security level and any defense project that is compromised, it can have grave and significant consequences to our national security. So that's one of the reasons why we process and handle data properly at various security levels. And BA systems has several solutions in place, and we work with other partners as well for cross domain solutions.

Jason Lopez:
The day, you know, many people in your field, keep coming back to the social piece of this.

Nandish Mattikalli:
Yup. And then, and that is very true. And, uh, we have seen, you know, these various fishing activities, right through social behavior and social engineering. It will just take clicking on one link that comes in my inbox. And next thing you know, that propagates to the network internally, what is more important for us is what we call APT the advanced persistent threat, that's significant interest to us. And how do we identify monitor, contain and react to those.

Jason Lopez:
So in, you know, designing and building apps for your clients, what are you looking at in terms of mounting a defense?

Nandish Mattikalli:
So, as I said earlier, talking about the apps, there is an implied reliance on the structure of the platform that it is secure, but at the same time, it takes a collaborative effort to communicate the needs of the security between various teams so that the security is built into the apps and the data at the applications layer and the data layer security features are built in not trying to add security on top. And then the dev ops concept we include application security, data security, and even security of some of these newer architecture, such as containers and hardening of the containers is a significant emphasis. And within the DOD, there are pre-approved containers and a use of pre-approved containers will help us get to the faster ATOs or even achieve continuous ATO. And BAE systems is investing. And we are working with various partners, including Nutanix and Dell, Microsoft, I believe with red hat as well. We are developing capabilities related to the security, especially in the cloud and the multi-cloud. And those are linked to zero trust automation of security implementation, and even continuous monitoring.

Jason Lopez:
Nandish Mattikalli is the chief engineer for the intelligence solutions business at BAE. This is the tech barometer podcast, I'm Jason Lopez. It comes to you from The Forecast and you can find us at theforecastbynutanix.com.