ceocfointerviews.com

Issue: January 11, 2021

Protect your Data, wherever it Resides

Sudesh Kumar
Founder and CEO

Kapalya
www.kapalya.com

Contact:
Sudesh Kumar
415-823-5440
sudesh@kapalya.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"While having cyber insurance you will be covered for the cost of recovery after a breach, but what about the intangible damage that was done to your company, to your brand name, and to your reputation, and how your customers will perceive you? It will be very difficult to gain their customer's trust and business. Using our solution, ensures that your data is protected and unreadable if copied by any cybercriminal." Sudesh Kumar

CEOCFO: Mr. Kumar, what is the vision behind Kapalya?
Mr. Kumar: When I started the company, I was a cyber security consultant working with the State of Hawaii's CIO and was assigned the responsibility of protecting the 2016 presidential elections data from getting breached. I recognized that there were many foreign government sponsored cyber criminals that were trying to infiltrate the election systems to steal voter registration data, which contains social security numbers, home addresses, phone numbers; basically, personal identifiable information. These data are people's livelihoods and their identity to society. Therefore, my mandate was to protect this data and that is where the idea for Kapalya was born. Kapalya's mission, our mission, is to make it as difficult as possible for cybercriminals to infiltrate, breach, and extract data regardless of where the data resides.

CEOCFO: How are you able to do it in a way that perhaps others have not recognized yet?
Mr. Kumar: What many companies do is what I call "prevention"; they are doing blocking and tackling. That means that they will say, "Let us see which avenue or angle the cybercriminal will penetrate my network, which way will they penetrate my servers, or which way will they penetrate my cloud account," and they start blocking and tackling there. However, there is a myriad of companies that are already doing that, but what is it that the cybercriminal objective at the end of the day? At the end of the day, the cybercriminal wants your data, because data is now the new "gold or oil". Data is valuable when it is interpretable. Therefore, one of the best ways to protect your data is to encrypt it. However, data encryption is only half of the solution. If you encrypt your data, you need a key to decrypt it. Now, if the key is readily available and cybercriminal can quickly find it, you will be compromised. That

means preserving and maintaining the keys for the data set becomes paramount. What we have found was that many companies are struggling to manage encryption keys for thousands or tens of thousands or even hundreds of thousands of users across multiple devices and geographical locations. It becomes a very daunting and challenging task. We are saying that we will encrypt all the data regardless of where it resides, then we will ensure that the way that we manage the keys is a different approach than what the industry is doing today, making our solution so much more superior to what is offered in the industry.

CEOCFO: Would you tell us about the unique approach?

Mr. Kumar: Absolutely. I will give you a very simple analogy. Generally, people have different keys for different things; you would have a key to get inside your office, a key drive your car and a key to open the door to your house. Those are three different keys. You do not want one key to open all three doors for you, because if this one key gets stolen -- now your office, your house and your car are compromised. We took the similar approach; that for every single file in every single folder for every single user on every one of their devices, we assign a different key. This means that the maximum damage a cybercriminal can do, if they steal your key, is compromise only one file. Let us consider you have one thousand files. The other nine hundred and ninety-nine files will not be compromised. The other mistake that most people do, and again I will use the same analogy, is they keep their keys with them. Chances are, right now, if you are walking on the street, your house key, your car keys and your office keys are all inside your purse. All is needed to get access to all three, is steal your purse. Therefore, we said, "let's not make the user keep the keys on any of the devices or any of the end points. We will give the key to the user when and only when the key is required." This is the other uniqueness to our approach; a unique key is assigned for every single file for every single user on every one of their devices, also we do not give them access to manage the keys. We give them the key to decrypt the file, then destroy the key from the user's device, making it extremely difficult for cyber criminals to steal the key. Other solutions have the key stored on the device which means your data is fully compromised if they obtain your device. However, with our approach, if a cybercriminal obtains and runs forensics on your device, they will never be able to find any keys. That is the uniqueness of our solution verses other solutions.

CEOCFO: How does someone get the key to a file they want to open?

Mr. Kumar: That is the secret sauce that we have developed, and our intellectual property. Essentially, we have
servers that are serving from private, public or hybrid cloud, so we serve the keys in real time. Kapalya agent would be running on your mobile or end-point device. Let say, you want to open an Excel spreadsheet. The normal behavior is that if you try to open an Excel spreadsheet, you just double click on that Excel spreadsheet and then the Excel program would launch, then the contents would launch, and you can start making your edits.

With Kapalya's solution, the user experience is exactly the same. You would double click on the Excel spreadsheet, but because the file is encrypted you need to decrypt the file before Excel launching the content. Once the file is double clicked on, the request is sent to our cloud service to say, "This is Lynn; she is coming from her laptop, she is a registered user and she wants to open this file called Excel123." Then in real time, we run our algorithms on our service to verify the following: 1. That is actually Lynn coming in and authenticate you. 2. You are coming from a device that is registered to you. Unless those two checks are passed successfully, and the particular file is legitimate, we will not give you the key. If all of those checks and tests are passed then, in real time, we go to a different server; i.e, where the keys are stored, which is a FIPS-2 compliant server, and we get the key. We encrypt the key, and then we create an encrypted tunnel between your device and our server, and we pass the key to your device. This is a double level of encryption for the key. Once the key gets to your device, it is decrypted, and we use the key to decrypt your file and then we destroy that key. That is basically the entire sequence. All of it sounds like it is going to be a very lengthy process, but we have optimized the algorithm so that the amount of time that it takes for you to double click and open an Excel file which is in plaintext, versus the amount of time that it takes you to double click and open an encrypted Excel file, is negligible. You will not see any difference. The only time you will see a difference is when the file is a very large video file, more than three hundred megabytes. Anything below, three hundred megs, there is hardly any difference.

CEOCFO: Can you open files from different devices?

Mr. Kumar: We allow each user to register up to five devices. It could be a combination of laptops, tablets, phones or even a virtual desktop environment. We offer two models for our services. First model, the company virtually buy all the servers and we would empower their systems administrators to then register the users. The company knows their users and the type of devices issued to their users, so the systems administrators would then register your device to the user profile. If your device is not registered, you will not be able to get any of the keys or do anything else. The second model is, where we would manage everything for the company. It is in a multi-tenanted managed services environment. For this model, you would send a request to us saying, "I bought a new phone" or "I got this new device and I would like to register it." We will take the information from device, and we will register it in the back-end system to the user profile and then and only then are you allowed to use the device.

CEOCFO: What types of companies, industries, sizes or geographies recognize what you are doing and are understanding and want to get involved?

Mr. Kumar: We started with state government, basically the public sector. Then we also started engaging with the Federal government. I was actually invited to present our solution inside the Pentagon last year personally. However, they wanted me to tweak my program based on their requirement, but they were very intrigued and very interested in it. That was basically where we started from and since then, we have

branched out to the private sector and the industries that we started targeting was the software services industry in Silicon Valley. Where we are finding a lot of traction is with other regions where they do not have access to public cloud services like Amazon Cloud, Google Cloud or Microsoft Azure Cloud. Where many cloud services provide, or offer their own services and they can offer encryption as a service, so they are embracing this service. We are signing up couple of those currently. We have not really hit the healthcare market yet, but the financial services are very excited about our solution. The legal companies and accounting firm are very excited about this because there are many sensitive documents that go back and forth and they want to ensure as much confidentially and protection as possible. Industries that have requirements to protect intellectual property, confidential, private information, personal health information or personally identifiable information, including government, are all prime targets for our solution.

CEOCFO: When you are speaking with the right person at a potential client, do they understand Kapalya? Is there an "aha moment" when someone listens and says, "Oh yes, we have to do that." What do you find when you are presenting Kapalya?

Mr. Kumar: The answer to that is "It depends." Usually, there are clients, like smaller companies, that do not really have an IT department, let alone having a security department. They say, "Yes, we get it, we understand that this is a requirement." The more sophisticated/technical savvy client that have large budgets and that have a large IT department; at first, are very skeptical, simply because, they say, "We already have all bases covered and our team has everything under control." Then I will say, "Give me another chance to explain and I will go through the details." Usually on the second or the third meeting, they really see how different our solution is, and what we are doing, verses what they already have existing in place. That is when they say, "Yes, this seems like something we would like to try." Those are the kinds of reactions that I have been getting most of the time.

CEOCFO: What is involved with implementation?

Mr. Kumar: Usually, we will sell them two different servers. One is our provisioning server and the second server is the key server. When I say server, it is a virtual server software license that they purchase; they can install them on their instance of any private, like, the Amazon AWS Cloud, or they can install it on their private could, inside their own data center. Then they install the agents across their endpoints; meaning all of their laptops, desktops, VDI and mobile apps on their smartphones and their tablets. Our solution pretty much takes care of everything.

CEOCFO: Would you tell us about your recent funding and how you will be using the money?

Mr. Kumar: We are pretty excited about this. The funding was not through a traditional VC. It came through a strategic investor, predominantly, in the United States, where they are very active in construction space. They work on very large projects, including building the new segment of the San Francisco, Oakland Bay Bridge in California.

However, in other parts of the world, they have a cyber security practice, and they saw Kapalya as one of the key elements that would complement their existing cyber security offerings. Once we started connecting to their customer base, they were able to see the excitement and the traction with their entire existing customer base. That is when they said, "You know what, we would like to make an investment and take share of the company, that way we are more closely aligned and then we will make this venture successful." That is the reason why they made the investment. The investment money will be used in two main areas. One is on the research and development on the engineering side to enhance our product and to build new features and to keep rolling out new versions with new feature sets that their customers are asking. The second, which is the most important one, is to really, ramp up our sales and marketing. That is because the sales and marketing budgets are huge and they take a long time to close deals, and that is where the bulk of the money would be going. Therefore, I would say that three quarters of the money will be going towards sales and marketing and closing customers and supporting those customers. The reminder of the fund will go to R&D, where we will be enhancing the product and rolling out new versions.

CEOCFO: What have you learned as more and more people are using your product?

Mr. Kumar: That is a great question. What I am initially finding is, that people have a poor sense of protection and that making me somewhat concerned. "I got this solution so I am protected," and I say, "Not really." When I go to the deeper conversation, and I explain to them that existing product only protects them only in one place and does not protect them all the way, that is when they light up. What I am finding out is that more and more people recognize cyber security as an essential business requirement, and that they need to invest on. I also recognize that they have bought all these solutions and implemented them, but I am finding that there is a false sense of security and they really need to understand more about the cyber security. I am educating them on where they are vulnerable and how they cyber criminals are actually using very sophisticated techniques including artificial intelligence to penetrate their systems and breach them, especially with ransomware. My biggest finding so far is that most people think that they are protected but that is a false sense of protection. Just because they get a compliance sheet from the government or whatever industry they are in, and they check that box to say, "I got that system, so I am protected." However, just because you checked a box from a compliance sheet, does not make you protected. You need to do all of these other details that are not provided by existing solution. That is what I am educating them on and that is why I am explaining them what our solution will do for them, to make sure that we are part of the last line of defense, when everything else has been penetrated and their bots steal your data. We say, "Go ahead and steal it, you will not be able to read it." Your data will be worthless to them.

CEOCFO: Do you see a point in the future when insurance companies or government agencies might require your system?

Mr. Kumar: Yes. Cyber insurance has become a major thing right now. Many companies are saying, "That is great that you have a solution, but I have cyber insurance, so if something happens it is not on me, it is the cyber insurance that is going to cover the cost." While having cyber insurance you will be covered for the cost of recovery after a breach, but what about the intangible damage that was done to your company, to your brand name, and to your reputation, and how your customers will perceive you? It will be very difficult to gain their customer's trust and business. Using our solution, ensures that your data is protected and unreadable if copied by any cybercriminal. Governments and insurance companies must recognize that there is a huge need for our solution and I am hoping that they will start partnering with us. I am not saying that they have to officially mandate something of this nature, but they need to recognize the real need for our solution and work very closely with us; absolutely.

CEOCFO: Why does Kapalya standout?

Mr. Kumar: It is simple. Everyone is, as I said, shouting prevention, prevention, prevention, but what they are doing is perimeter defense. The market is crowded, there is too much noise and generally speaking, enterprises and consumers are confused. Our message is, we know what the cybercriminal are looking for; your data. How do we protect your data? By encrypting it. How do we manage the encryption keys? By using a very innovative technique that we have developed. Therefore, we have cut the chase of giving you fancy cyber-attack prevention diagrams, or fancy multi-factor passwords or anything else like that. We have cut through all of that and we are getting down to the core to protect what the cybercriminal is after, your data. If the cybercriminal wants is your data, why do you not just protect your data? That is what is the key differentiator between us and what the other guys are doing. The other guys are saying, "We can do data protection; doing data protection this way or doing data protection that way," and everybody understand that encrypting data has been around for hundreds of years. In World War II, all transmission was encrypted. Decades ago, data transferred through the internet use to be in plaintext. Now days, most data transfers are encrypted. Decades ago, stationary data was in plaintext. Today, most of data at rest are still in plaintext or can be easily decrypted with a single key. Our solution challenges this convention for the protection of data. That is the most basic fundamental thing you can do. However, encrypting is one thing, and key management is a different thing. How do you manage keys for all of those files? That is what we have cracked and that is very difficult to do and that is what I am trying to tell these people; that at the most fundamental level; yes, you have got a lot of defense systems, and yes, you have got Artificial Intelligence, and all of those things are fine, but if an attack is mounted from your office without your knowledge, the attacker has only one thing in mind; getting your data. That is basically where we are. That is basically what we protect and we make sure that even if they make a copy of your data, they cannot read it. That is the reason why we are different than all of the slew of other companies that are offering.