ceocfointerviews.com

Issue: June 7, 2021

Airgap Stops Ransomware with Ransomware Kill Switch™

Ritesh Agrawal
CEO

Airgap

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Agrawal, what is Airgap?***

Mr. Agrawal: Airgap is ransomware protection company. We're in the business of protecting our customers from the menace of ransomware attacks.

CEOCFO: ***What is your approach to handling ransomware***?

Mr. Agrawal: There are some fundamental flaws that are not being addressed by any of the vendors in the industry. That is why we are seeing such a massive growth of ransomware across the board. Based on my career and research in network security over the last 10 years, and my 25+ years in computer networking, I isolated those flaws and designed a very potent solution to correct them.

Our customers are super excited about what we have to offer, our investors are excited about the prospects of Airgap and of course the technical members of our team are just as excited about solving a very big problem for the industry.

CEOCFO: ***Would you go into a little bit of what the flaws are and how you can alleviate them? What are the problems and how can you fix them?***

Mr. Agrawal: The fundamental issues are twofold

One is that there is too much access from one particular device to other devices inside the organization. For example, if you and your colleagues are sitting in the same office, in theory you can all talk to each other without any control whatsoever. But that also means that if one of your laptops is infected, it can easily infect other laptops or printers and vice versa.

The other fundamental flaw is this presumption that I need to protect the perimeter, as if to lock my house from outside, and then once anyone is inside, that person can roam around and have full access to the inside of the house. This is exactly how enterprise networks still operate.

These days, people take their laptops home, they work from home or from public hot spots. They could potentially infect their laptop and bring it to the office. For that case, perimeter protection does not help much.

Airgap's approach is to assume the perimeter is breached and to restrict the natural movement of bad actors inside the organization. That's something nobody else is addressing.

CEOCFO: ***How does the Zero Trust Isolation™ platform work?***

Mr. Agrawal: The whole idea of Zero Trust Isolation™ is to ensure that every communication is authorized first and authenticated next. If you are trying to communicate with me or anything else, I need to make sure you have the authorization to do so.

For instance, if you have access to your Gmail account you are authorized to access your Gmail account, but you will not get access unless you authenticate yourself—you must enter your login and password. Similarly, Airgap makes sure that you are first authorized and then authenticated. That is what we are calling Zero Trust Isolation.

CEOCFO: ***Are people annoyed at having to do a secondary level or is it becoming commonplace?***

Mr. Agrawal: That's a very good question! Security always involves a little bit more work. Ideally, we would like to avoid that work.

We have some very interesting mechanism to detect suspicious behaviors anywhere inside the organization. When we do, then we go into this lockdown mode where we ask everyone to authenticate themselves multiple times before they are granted access. This is only when certain conditions are met, when we think there is a threat inside the environment, and at that time nobody complains, because they understand that this is all for the better protection of the enterprise itself.

"With the Ransomware Kill Switch, we instantly shut down all unauthorized and unauthenticated communication and thus limit the exposure of ransomware inside your organization. That is something that our customers are super excited about." Ritesh Agrawal

More importantly, we also have this Ransomware Kill Switch™. We know that one day or someday, everybody is going to get infected and when that happens people do not have an appropriate method to protect themselves. I have had CIOs tell me that they watched the house burn down, because what can you do? You see that someone is propagating and you cannot do anything.

With the Ransomware Kill Switch, we instantly shut down all unauthorized and unauthenticated communication and thus limit the exposure of ransomware inside your organization. That is something that our customers are super excited about as well.

CEOCFO: ***How have you developed your Ransomware Kill Switch™?***

Mr. Agrawal: Honestly, I would not take the credit. This was from feedback from a customer, turning to us for technical innovation. The customer basically said, "You have a great product that protects against ransomware to begin with, but what if that human error happens, someone misconfigures your device or something happens and now I am under a ransomware attack. What am I going to do?" That kind of sparked the discussion of, "What would you like to do?" They said, "It would be nice to have a ransomware kill switch."

Then we started noodling on the white board, coming up with ideas as we always do. We tested the idea, then productized it and now we have it deployed it across dozens of customers. The way it works is that we carefully inspect and monitor all communication patterns. If you tell us that there is ransomware inside the organization, or if we detect its presence, we go into what we call a lockdown mode. In lockdown, you only need necessary and authenticated communications. Everything else is locked down. This would include communications to conduits, like a storage system, your backup system, your customer data, or your employee driver data.

So we lock down what enterprises call their crown jewels, and we eliminate all unauthorized or unnecessary communications. For example, you may have rules that allow video streaming such as photographs, TV or a home security system. When you're under a ransomware attack, that's not a very important task.

We start eliminating those unimportant tasks, because hackers are going to figure out a way around and leverage some of these communication mechanisms to impact you. We essentially shut down their ways to get to other systems.

CEOCFO: ***How do you reach out to potential customers? How do you alleviate some of the skepticism?***

Mr. Agrawal: There are a couple of questions in here. One is how to we reach out and the second is how we address the skepticism.

I will tell you the first one. First, we have a great network of our friends. In addition, our customers are recommending other customers now, so that is great for us! There are industry newsletters. There are LinkedIn outreach programs that we have. We reach out to CSOs and CIOs, explaining to them what we have to offer. The good news for us is that everyone is familiar with ransomware and to an extent, everyone is somewhat affected by it. Therefore, when we reach out with details about our program and our solutions, we often get an audience and when they hear our story they love it! That is our outreach program so far: our network, our investors' network, and LinkedIn.

In terms of skepticism, some of our customers are bombarded with messages from many vendors that claim to do the same thing, so the first reaction is that it must be too good to be true. But when we describe the technology in detail, we see an almost instant conversion to fandom. Everyone thinks we have a great solution and that this is the right approach to solving the industry's problem. Our vision is based on making a fundamental change in the way that enterprise infrastructure has been deployed and delivered, and our future is very bright. With help and guidance from our customers, we could be an important company in the valley.

CEOCFO: ***What is your geographic reach today?***

Mr. Agrawal: Well, ransomware does not discriminate! It affects everyone equally. That is what I've learned in the last eight months of talking to customers. Pretty much everyone in every geography is impacted. Most of our customers are in the US. We have some in Europe and we have a few in Asia, Australia and some in Southeast Asia. So pretty much everywhere. Everywhere there is ransomware there is a need for Airgap.

CEOCFO: ***What surprised you from concept to where you are today at Airgap?***

Mr. Agrawal: When I started the company, I knew there were problems in the industry—I could see the fundamental flaws. Once I figured out the solution, it was hard to resist the temptation to start a company. I'm surrounded by great investors, very good advisors, a wonderful family and good friends. They all supported me in this effort. But I didn't imagine we would get this much excitement, this quickly from our customers! If I had foreseen this, I might have started earlier. We're excited about what's happening.

The second thing that surprised me is that I hadn't imagined it would be so much fun! Of course, I'm still making much less money and working quite a bit harder than I was before. But I'm enjoying every minute of it. Those are two surprises: the amount of fun and the early success.

CEOCFO: ***Are you seeking partnerships, investments, or funding as you move forward?***

Mr. Agrawal: Absolutely! We're always seeking partnerships. No company is an island in this industry. We definitely need a partner ecosystem. We're building a very important platform and we'd like everyone to partner with us, from the technology side to the services sector side. We're working with dozens of partners already and would like to add more to our portfolio.

We can make a fundamental difference in the way the enterprise is architected. The current blueprint of the enterprise is at least three decades old. That needs to be revamped. Someone has to do it. Why not Airgap? I would like to welcome conversations with prospective investors that have visions for the future, that are willing to partner with entrepreneurs like ourselves and work with us to build something great.

CEOCFO: ***What, if anything, might someone miss when they are looking at Airgap, whether from a usage, partnership, or investment perspective?***

Mr. Agrawal: That is a great question. If you go to our website, clearly, we cannot describe all the gory details of how things work, where the future and the vision of the company is. Some of this is confidential, and some are just things that we think it is better to discuss one on one with customers, prospects or investors.

So you look at our website and see that we are solving one problem—ransomware—because we solve it so well and that is bringing us a lot of business. But give us a chance we'll describe not only other problems that we're solving and how clever our solution is, but we'll also let you know more about the company vision. Once people understand that, they're often as excited as we are.