"WE ARE TRYING TO BE THE SINGLE PANE OF GLASS FOR LARGE ENTERPRISES"

Srinivas Rao, Co-Founder and CEO of Aujas Networks traces its origin and elaborates on its solution portfolio

Jyoti Bhagat
jyotib@cybermedia.co.in

What has been the origin of Aujas and how has it evolved over the years?

We started in 2008 and have completed 10 years. Primarily when we set up the business, we felt that this space of cyber security is underserved. There were not too many people who were focused on this. In fact, it still is. There are obviously a lot of large product companies; however the services were kind of neglected. We felt there was a market opportunity for us to leverage. Cyber security was going to be more and more critical and would become a kind of de facto requirement.

If you analyze that within cyber security, there are some companies who are playing out on the perimeter level and some with identity

management. What initially was the focus of Aujas?

When we set out, we said we want to help people protect identities, applications and data. That was our premise and essentially the intent was to ensure we help organizations to manage and mitigate IT risks. We started off focused on Professional Services. Our foundational service includes risk and compliance, identity & access management and threat management services. These are the three primary focus areas of Aujas. We have also added some new capabilities; we introduced security intelligence and operations, in the last 12 months, we have added security engineering services and digital security.

Typically each of our service lines would have consultancy, deployment, sustenance and optimization piece. We have strategy and design which typically consultative, and then we have implementation/deployment, which is to rollout program and third part is sustenance. For example, if you are undertaking a data protection program, we would first undertake a consultative exercise in terms of Identification of data, data flow analysis, data classification rules. After which we deploy the DLP tool which could be a commercially off the shelf tool. Then there is the optimization, which is how you make the data protection program truly effective and deliver outcomes.

More recently in the last 12 months, we added two new services one of which is Digital Security and the other is Security Engineering. API economy is one such area in which digital security is crucial. For example, if you are a travel portal you need to integrate with banks, payment gateways and so on. The entire information exchange is done through the API. Since securing those API have become a big issue, we built a solid practice today around API security. Secondly, we are also doing a few pilots around Security on Private Block chain for Banks in areas like remittances.

And across your services, do you work with all vendors?

We tend to be vendor neutral; we are not biased to any particular vendor. However, having said that, there are some partners who we work with a little bit more. For example, in the risk advisory space, we tend to do a lot of work with Archer from RSA. In the Identity and Access space we have done a lot of work with IBM, CA and with Sailpoint. Similarly, in the security intelligence and operations space, we've worked with IBM and RSA.

What kind of use cases, or deployments in security do you do?

What we are doing is, just like in the app world. When you say App world, if you take your hand held device, everything is emerging in the form of apps. Similar shifts are taking place in security space. If you look at the large vendors, whether it is an IBM, or whether it is Splunk, etc, they are trying to become a single source of truth. So for example if you take IBM, they have this platform known as QRadar. One of the things they are trying to do is ensure this become the single pane of glass for large enterprises which multiple point tools within the enterprise. For example, if you have an end point detection & response tool, data leak prevention tool, or if you have a threat-hunting platform, how do you integrate what this tool does into the primary platform which is the SIEM / SA Platform. We are actually in doing lot of security engineering work with product vendors integrating their platforms with the larger, SIEM / Security Analytics Platform like Splunk and QRadar.

We have done about a dozen deployments here with organizations who have built DLP (Data Loss Protection) tools, threat-hunting platforms taking those platforms and integrating with SIEM / SA Platform like IBM QRadar and Splunk. These are large product vendors, so we are doing the equivalent of OPD work, but purely focused on security.

SRINIVAS RAO,
Co-Founder & CEO,
Aujas Networks