

THE POST-PANDEMIC WORLD RESHAPING THE SECURITY CHALLENGES

PLUS, THERE ARE MANY ADVANTAGES IN STORING DATA CENTRALLY AND OFF-PREMISE WHEN IT COMES TO MOBILITY, REMOTE WORKING, COLLABORATION, AND FLEXIBILITY. MANY ORGANISATIONS PREFER THE COMBINATION OF BOTH CLOUD AND EDGE COMPUTING SUITS. AT THE SAME TIME, SOME BUSINESSES OPT FOR THE NETWORKING ARCHITECTURE KNOWN AS FOG COMPUTING, WHEREBY INSTEAD OF COLLECTING AND ANALYSING THEIR DATA IN 'THE' CLOUD, OR AT THE EDGE, IT IS HOSTED ON A LOCAL AREA NETWORK.

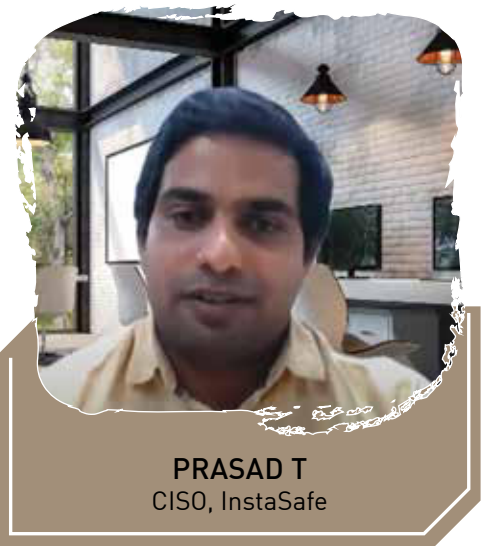
The advantage of edge solutions includes low latency, high bandwidth, device processing and data offload as well as trusted computing and storage. Cloud solutions are often cheaper, more powerful, easier to implement, integrate, scale and shift the cost burden from capital to operational expenditure. Plus, there are many advantages in storing data centrally and off-premise when it comes to mobility, remote working, collaboration, and flexibility.

Many organisations prefer the combination of both cloud and edge computing suits. At the same time, some businesses opt for the networking architecture known as fog computing, whereby instead of collecting and analysing their data in 'the' cloud, or at the edge, it is hosted on a local area network. On this backdrop VARINDIA has recently hosted an

event on the importance of cloud, importance of hybrid computing in reshaping the corporate data centre, on cyber-crimes etc. The event was moderated by Dr. Deepak Kumar Sahu, Chief Editor, VarIndia.

On the importance of cloud, Prasad T, CISO, InstaSafe says, "Initially, it is becoming a big challenge to the cloud technologies organizations, because data is very costly. So, even one security threat can cost millions for companies. Technology is coming up to protect these. Companies are moving to cloud because of scalable factors and the cost can scale to any mode dynamically on the requirement basis, and then scale down and pay only for what is used. Due to this capability, more hybrid capable solutions are getting in the cloud and beyond. At the same time, security post shows also need to be taken care of, that is like the biggest challenge today. I would also say zero trust here because I am hearing it daily. These kinds of technologies of protecting the assets of the organizations are being watched from outside. Today, we have a lot of automated boards running around. So as long as we have a proper protection in place, then I think it is completely possible. Cloud is the way to go, what I would suggest, that it is the future, this is the place where we can do a lot more innovative and use resources only when we need."

On cloud infrastructure he also depicts, "According to me, there are two angles, one how your cloud infrastructure is structured and configured because the cloud has its own way of getting into and way of hacking. They have their own ways. There are security policies, DPC configurations and stuff. Each cloud has its own settings and other things. Once you remove that layer, then it is the same as the Data Center. You



MODERATED BY





VIVEK AHUJA
Head-IT, IDEMIA



BHARAT B ANAND
Head It & Security- EC Council



ADVOCATE DATTATRAY
B. DHAINJE

have your service application so that the same way you keep it in the data center, however the security posture of these is the responsibility of the company. Many believe, once you move your infrastructure into the cloud that is the cloud provider's responsibility to take care of it. That is not true. Make sure whatever you want, even in your data center for that matter, get it tested by some security researchers and have your own routine of scanning policies, you have in place, and if you can keep them behind a firewall gateway."

On the importance of edge over hybrid cloud Vivek Ahuja, Head-IT, IDEMIA says, "It is not very easy for an enterprise but it is easy for a startup, as it can be born in the cloud. But for the enterprise it is a game. For some government projects and some private banking projects it worked well. Whenever they want to ramp up, we can do that within minutes. If we had purchased the hardware in our data center we could have never maintained that business. Hybrid computing, and choosing where to use the cloud or not to use it is very important.

From my point of view, software defined networks are used when we look at security or lateral blocking of traffic or monitoring of it but if we look vertical my experience is not very nice so far. We have used software defined networks for regular traffic and as well as for vertical traffic also, with options from virtualization providers."

Talking on the importance of edge over hybrid cloud, Bharat B Anand, Head It & Security- EC Council points out, "People are right now looking at a combination of both, hybrid and cloud because of regulatory for one reason, and the second industry to industry. This is a transitional phase before we have probably a time to count where they compromise changes to hybrid to serverless. Probably more people have started talking about serverless architecture. If you look at reports by Gartner or IDC, you will see those who have been talking about on-premise have transitioned to hybrid. And those who have gone hybrid about 60% of them and started talking about how to go into the serverless architecture.

For sure, technology innovation brings in

a lot of use cases, in terms of availability, ease of doing business on and so forth, the most important one is the pandemic, which acted as a catalyst.

When the lockdown happened and people had to be augmented, then the business came really handy. Most of Microsoft or AWS is a clear indicator of this while the rest of the businesses took a hit. Major shift is happening and it is going to happen, as the organizations will start looking at their business from a business-focused point of view, rather than an IT-focused point of view. My core business is to manufacture automobiles, So I will be focused on how to deliver a positive management system, which should have inherent limitations of saying so, so I would prefer, and move into a space where I have anytime, anywhere availability."

Whereas, Guru Prasad Rath, Business Analyst & Senior Advisor - Applications focuses on the challenges of cloud, he comments, "Being a person from the application, I find the biggest challenge is the cyclic use of data. And when you move to the cloud, how much the data is being used, particularly an industry like FinTech or BPO look at a simple example where the invoice image needs to be downloaded a number of times for verification, modification and data entry, the cost of cloud becomes more.



GURU PRASAD RATH
CTO - Fenexa Technology

When We shifted from on premises to the cloud, we got a bill almost double. Optimizing the usage and the cyclic use of data is of great challenge. As cyclic use of data is more particular, clients have to look at how to optimize the implemented product."

On the rising cybercrimes and to decipher away from it, Pankaj Khare, HEAD-IT, PINE LAB elaborates, "We may or may not gain the immediate benefit from cloud computing. Definitely one has to take security measures. I would say that are data breaches, applications via cloud, but by having proper security controls in place we can have it in our hands.

There are so many authentication layers while using cards. As I work for Fintech, we ensure that all the CVV numbers are confidential whenever we secure, we have to follow the norms of changing the password and the pin regularly.

These are some basic things I would suggest one should do in order to avoid the vulnerability of using cards, and we should never use the systems which is kind of remote and vulnerable, because we need to have a proper system, even the mobile devices, by which we are using anything related with our financial transactions should be properly secured enough. That is the point number one. Changing passwords, pin numbers regularly is a secondary option."

Representing the common man's interest Advocate Dattatray B. Dhainje raises concern for the cloud-based environment and its challenges. He says, "Multi-factor authentication is a beautiful way in which we can detain the security. Crypto-jacking is like a cyber security challenge which might occur in a cloud-based environment. Many have experienced data breaches, hijacking accounts even when people are using the cloud.

Training is also an important factor in providing cloud security. If we want to make sure that our cloud-based environment needs to be secured then ideas like intrusion detection systems, intrusion prevention systems are the basic dividers."

The event ended here with a happy note. ■