Nubeva
Frequently Asked Questions

Nubeva was born in the cloud for the cloud to make security in the public cloud available everywhere, for everyone; and to make it better, faster and more affordable. Randy Chou co-founded Nubeva in 2017 and created a team that built a blueprint to unlock the potential for running security in the cloud. Today, the company is linking the best security technologies with public cloud platforms so enterprises can maximize their use of the cloud and get quick, easy access to the packet traffic they need with confidence.

What does Nubeva make for the public cloud?
Nubeva created Nubeva Prisms. Prisms allow organizations to gain more visibility of their packet traffic in the public cloud. Prisms are essentially agents that tap, mirror, aggregate, filter, process and replicate packet level traffic from virtual machines and containers in any public cloud. Prisms send processed packet feeds to multiple tools and services both in-cloud and on-premises. With Nubeva Prisms, users can activate and run the tools of their choice to gain the critical visibility and control they need. Enterprises use Prisms to accelerate their cloud transformations with clarity and confidence.

How does Nubeva ensure security in the public cloud?
Organizations know they can't apply legacy data center approaches to security in the public cloud. Chokepoint tapping, pre-defining endpoints and network edges for monitoring are legacy data center architectures that, if forced onto the cloud, end up nerfing the cloud.
- Security, DevOps and high availability teams must treat everything in the cloud as an individual resource, implement policy-driven solutions that automatically include new cloud resources as they spin up and spin down, and make use of cloud native capabilities that don't interrupt and disrupt the applications and operating systems they're supposed to protect.
- Nubeva Prisms does this by acquiring packet-level traffic from virtual machines, containers and other elements of the public cloud. And Nubeva Prisms scales automatically, based on rules and criteria triggers as additional elastic sources come on line.
- Prisms' container-based Packet Services Processor uses native cloud container solutions for dynamic scalability as the amount of traffic in the system increases. Nubeva can also ensure that your tools can scale as well by load-balancing replication to any number of destinations.

Don't the big public cloud providers offer visibility into packet traffic?
Public cloud platforms offer preventative security. Unfortunately, that's only half the battle. Figuring out what happened when a breach occurs is more difficult than simply patching a vulnerability after the fact. Large public cloud providers share logs, which provide a partial answer. Flow records may offer additional insight. **But the vital piece of the triad is the aggregation, processing, storage and distribution of actual packet level data.** Full packet capture is absolutely critical for forensic investigation. This data is the best asset for troubleshooting and root cause identification. Need to know exactly what happened last night

at 11:55 p.m.? Pull the actual traffic and replay it using security tools. If a specific security event happened in the last seven days, organizations must have access to the complete data haystack in order to find the appropriate needle.

Why is it important to see this detail in the public cloud?
If organizations can't quickly and accurately see what's going on across their public cloud environment at all times, they run the risk of not knowing when they're being attacked or compromised. Continuous traffic visibility inside the cloud, and the ability to "insert" security control points, is the key. These are critical steps toward improving security, especially when dealing with the dynamic, elastic nature of modern cloud computing environments.

What does the future hold as more organizations move to the public cloud?
For organizations with strong confidence and proven applications already riding on public clouds, adopting a cloud-first strategy for all IT decision making will become the norm. Cloud first is simply a tech philosophy designed to maximize AWS and Microsoft Azure as a core business strategy. Cloud offers organizations the ability to keep servers up no matter what, so critical business operations aren't using up valuable resources for maintenance, updates, upgrades and infrastructure expansion demands. As cloud migration becomes the norm, organizations will demand simplicity and high-performance that matches their experience in traditional data centers. This means moving security to the cloud, which means tapping a solution that provides the right level of access, visibility and control of critical packet streams.

Nubeva is a cybersecurity SaaS software developer for enterprises with public cloud assets, listed in the TSX Venture Exchange ("TSXV) in Canada under the ticker symbol "NBVA".

For more information: www.nubeva.com or email at info@nubeva.com