NUBEVA

PACKET SECURITY IN THE PUBLIC CLOUD

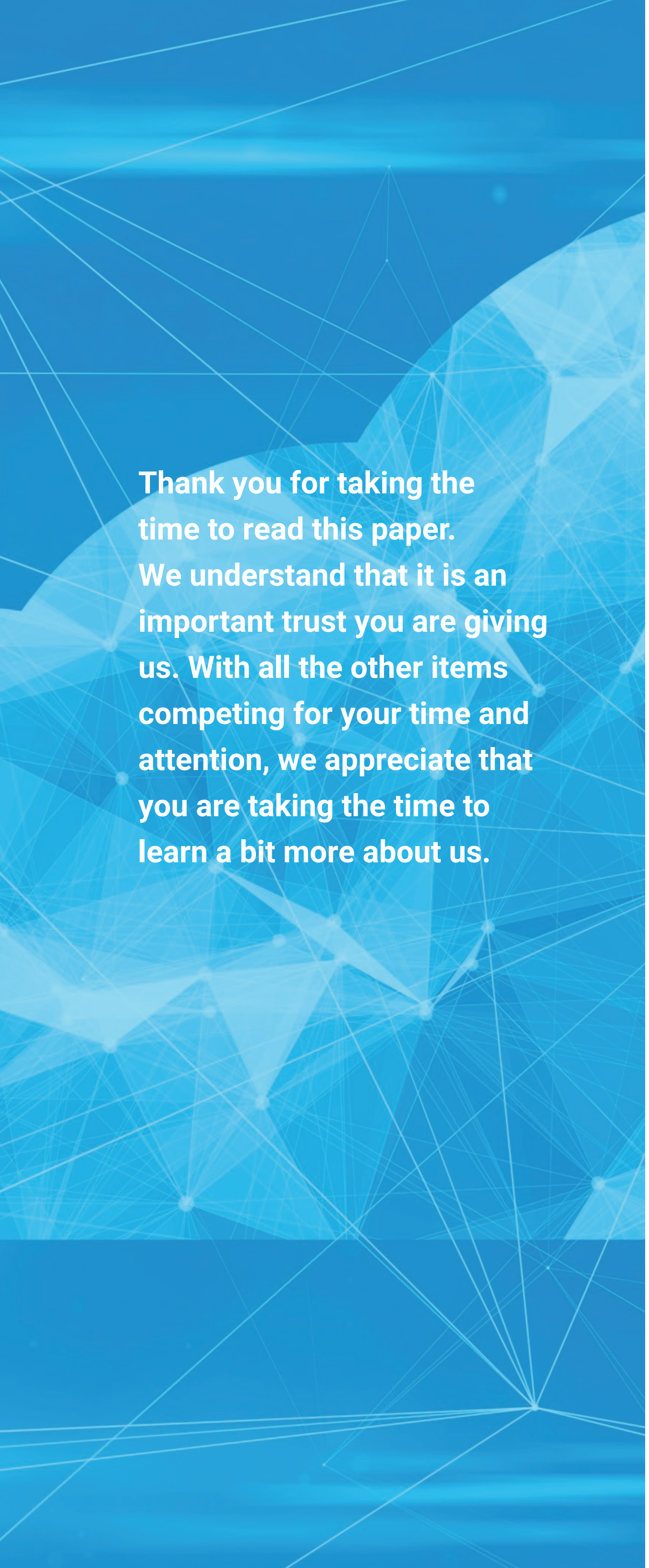
Contents

Author's Note 3

The Cloud Is Different 4

Solving The Cloud Dilemma 8

The Nubeva Difference 14



Thank you for taking the time to read this paper. We understand that it is an important trust you are giving us. With all the other items competing for your time and attention, we appreciate that you are taking the time to learn a bit more about us.

Author’s Note

WE ARE FOUNDED AROUND 3 CORE PILLARS OF BELIEF:

1

Activate Cloud Adoption by Enabling Security

The future of business is the cloud and securing the cloud will be a vital initiative to activate their business in the cloud. Nubeva enables organizations to deliver security everywhere both in-cloud and off-cloud.

2

Support Technology Choice

Best of breed means something different to each organization. Organizations select technologies, build technology stacks and rip and replace based on business requirements and technology innovations in the marketplace. Nubeva is committed to supporting our customers, regardless of what tools, processes and expertise they have selected.

3

Provide Affordable Solutions

To provides best of breed security for all, the solution must be affordable. The cloud is the global IT delivery platform of the future. The cloud allows commoditized computing with simple services. As Nubeva is a cloud service full born in the cloud, we maintain the promise of affordability in order to provide best-of-breed solutions to all.

The Cloud Is Different

In traditional environments you have physical access to your data centers. IT teams can access the racks and stacks of servers to feed their tools with packet traffic from physical TAP and SPAN ports, optical mirroring and big network packet brokers sitting along side the servers they watch. In the on-premises world, cables and tables connect the systems we need with the tools we trust.

SECURITY, MONITORING AND COMPLIANCE REQUIRE PACKET TRAFFIC. COMMON IN THE DATA CENTER, PACKET ACCESS IS SCARCE IN THE PUBLIC CLOUD.

Today, business moves at the speed of light. Information travels between servers and applications between employees and customers The systems you depend on, need a constant feed of data to ensure security, to guarantee uptime and to keep the information moving.

In traditional data centers, organizations track, monitor and secure their environments. They have security tools, network and application monitoring tool sets. These represent large investments in both technology and teams. There is significant time and money spend on creating, training and optimizing the processes used by these teams and supported by these tools. This is what keeps the organization running and secure.

To keep these tools, teams and processes running, organizations use specialized infrastructure like network TAPs and SPAN ports to access packet traffic from their applications and network nodes and replicate it to the monitoring, diagnostic and security tools they use. Those tools perform deep analysis, detect anomalies and identify areas for optimization. Teams respond to optimize and secure the business.

All this changes when companies transition to the public cloud.

The cloud has eliminated the network intersections we once monitored. The cloud has evaporated the network edges we needed to guard. As a result, we starve the tools and teams of the packet traffic they require to detect, protect and optimize.

WHEN COMPANIES MOVE TO THE PUBLIC CLOUD, THEY QUICKLY REALIZE THAT THEIR DATA CENTER APPROACH TO SECURITY, MONITORING AND COMPLIANCE DOESN’T WORK.

The public cloud makes use of virtualized resources that do not allow the same kinds of packet level access that are commonly available in your own data center. The cloud also introduces new kinds of resources that are ephemeral in nature. They pop into and out of existence quickly and only as needed. Additionally, companies do not have the burden of hardware and network oversight. They can focus on their core business while the cloud service providers like Amazon AWS, Microsoft Azure and others focus on keeping the infrastructure running. Indeed, these are several of the key advantages of the public cloud.

These advantages come at a cost: you no longer have control of the network. The network is hidden from you. The cloud companies do not provide you with the kinds of access that you had in your data center.

The result is that the tools and teams and processes that you developed to run and secure your business lack key elements. They lack:

- packet level access to what is going on in the public cloud.
- packet level data feeds that they inspect for security.
- packet traffic they analyze for unusual behavior.
- packet information they capture and index for compliance, investigation and replay.

0 1 0 0
0 0 0 0
1 0 1 1

73%

of organizations are operating with uncertainty about the status of their data.

Source: 2018: State of Virtualization in the Cloud by Druva

THE PUBLIC CLOUD PACKET DEFICIT LEADS TO TWO COMMON APPROACHES AND ONE TYPICAL OUTCOME.

FIRST

In their shift to the cloud, some organizations choose to eliminate security, visibility and monitoring at the packet level. They may even be advised to dump their tools and teams that require packet traffic to properly function. They accelerate their adoption of the public cloud and hope that nothing bad happens while at the same time, hoping someone else solves the problem later. The motivating idea is that the cloud providers like Amazon, Microsoft and Google are big enough to keep them secure.

SECOND

Organizations who know that they must do something but are unsure what to do drive the second approach. They understand that the cloud service providers do not guarantee security and that they, the organization, have some skin in the game.

So they try to cobble something together with their legacy vendors. But these solutions are expensive, incomplete and build around legacy, data center thinking instead of a cloud-first mentality. These systems are incredibly high cost and introduce interruptions in computing, administration and capacity – the very things they're supposed to help avoid! It's like being forced to buy tires that are more expensive than the car!

Last year, (2018), the 60% of enterprises that implemented appropriate cloud visibility and control tools experienced

ONE-THIRD FEWER SECURITY FAILURES.

Source: "Is the Cloud Secure," by Kasey Panetta, Gartner Inc.

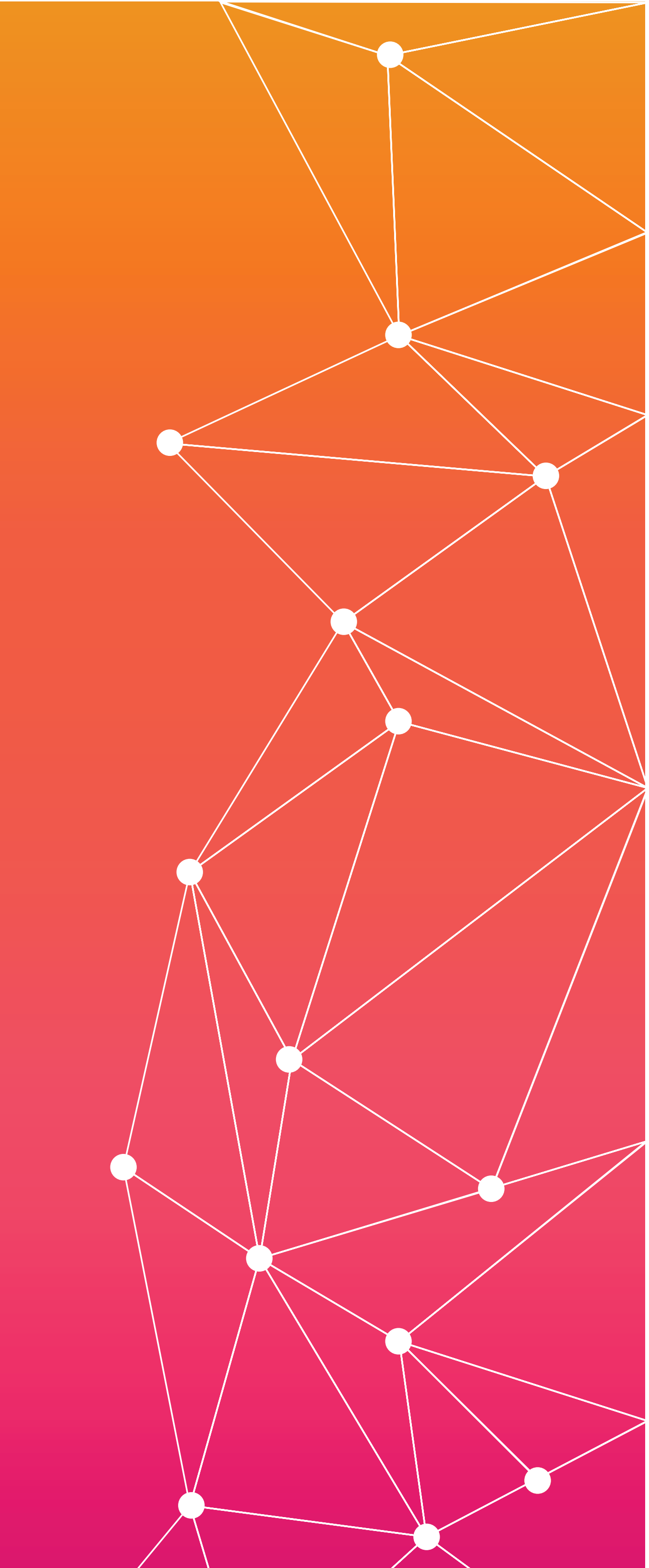
THE DILEMMA OF THE PUBLIC CLOUD IS THAT COMPANIES HAVE LESS VISIBILITY AND SECURITY THAN THEY DO IN THEIR OWN DATA CENTERS.

Unfortunately, there is one typical outcome for both of these approaches. And that is, organizations end up with less visibility and less security in the cloud than they have in their own data centers. They are flying blind.

This, then is the dilemma. How do you gain all the advantages of cost, convenience and elasticity of the cloud while maintaining your security and performance posture? How do you acquire, process and distribute cloud packet traffic to your security and monitoring tools, teams and processes?

This is where the rubber meets the road: what if you could move immediately into the public cloud AND ensure your tools and teams had all the packet level data they need to keep your business moving at the speed of light?

This is exactly what Nubeva Prisms is designed to solve. It restores packet level visibility and control to get cloud packet traffic to your tools, teams and processes so you have the same level of control over your cloud environment as you do over your data center environment.



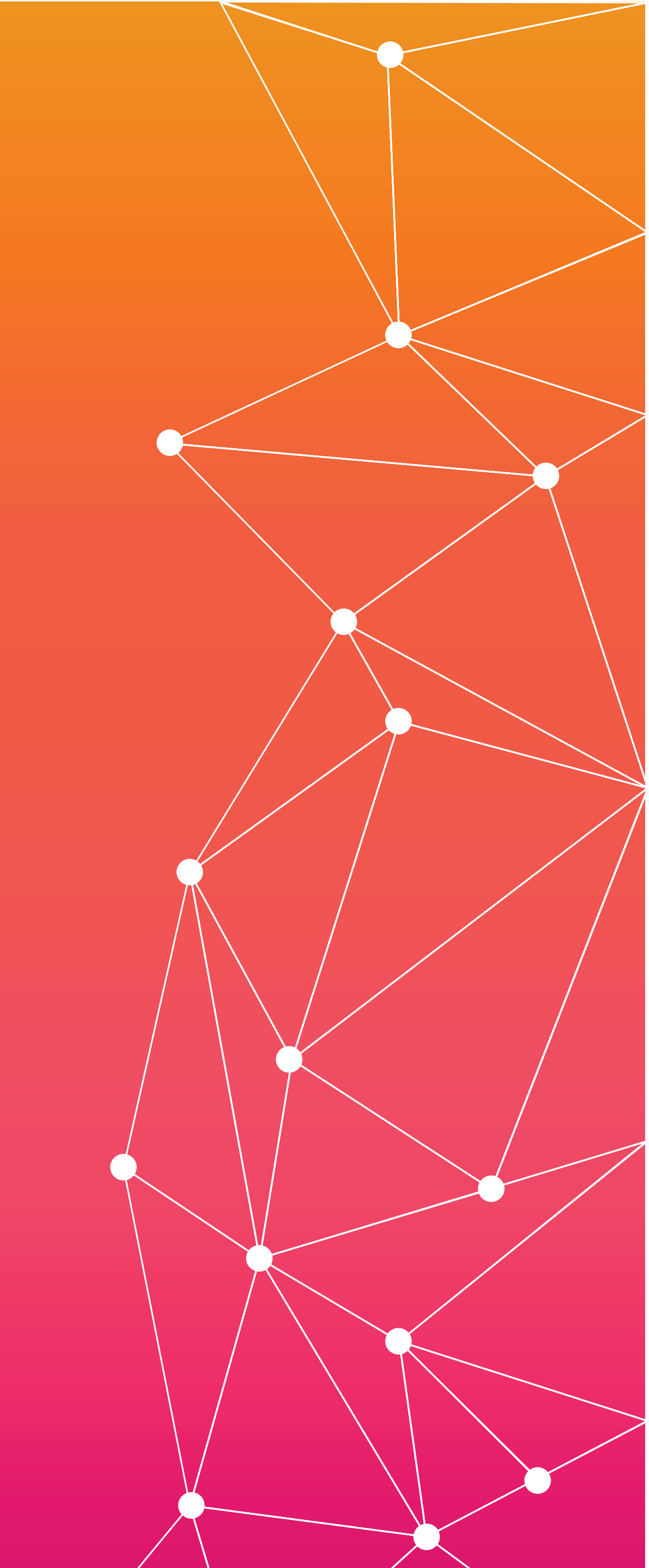
Solving The Cloud Dilemma

NUBEVA PRISMS DELIVER FILTERED CLOUD PACKET TRAFFIC TO TEAMS AND TOOLS.

A born-in-the-cloud solution, Nubeva Prisms get cloud packets to your existing teams and tools.

Instead of breaking the bank for partial visibility or dumping your teams and tools, Nubeva Prisms actually increases your ROI by feeding your existing security, application monitoring, network monitoring and compliance tools with packet traffic from your cloud systems. This extends the lifetime and effective use of the investments you've already made without sacrificing learning and ramping time for the creation, education and rollout of new teams, tools and processes.

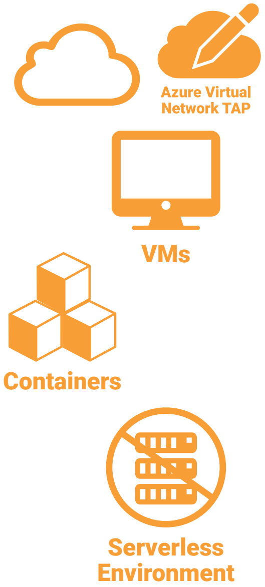
This is how it works.>>



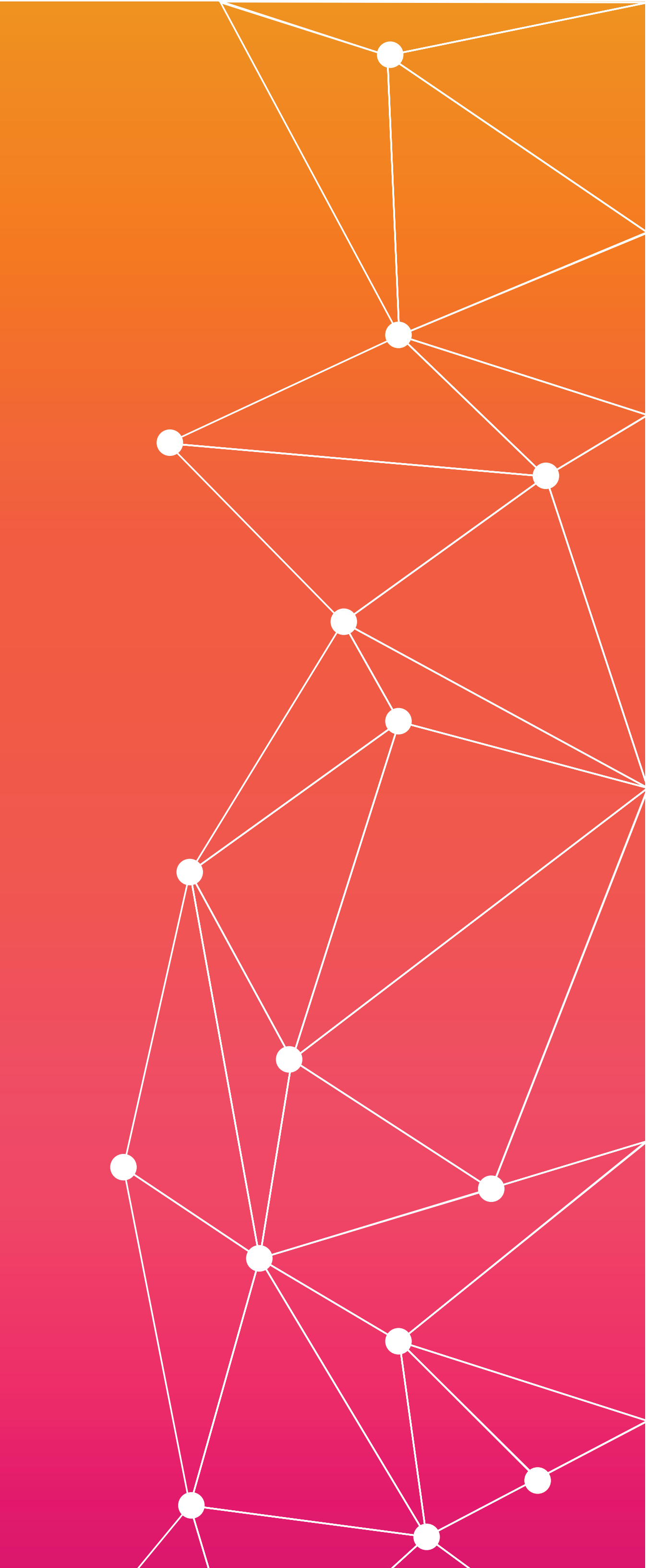
NUBEVA PRISMS DELIVERS ADVANCED PACKET ACQUISITION WITH CLOUD NATIVE ARCHITECTURE.

In your cloud environment you have many different kinds of resources. You have virtual machines, containers and container clusters. And serverless is on the horizon as well. All these systems are generating traffic. They're generating north-south traffic in and out of the clouds as well as east-west in between the applications and peered regions. This traffic is your data in motion that needs to be monitored.

To do that Nubeva provides the most advanced and complete ability to acquire this traffic. Prisms support native cloud infrastructure capabilities like Azure's VTAP capability. Where native public cloud tapping infrastructure is not available, we deploy our Prisms sensor which is next-generation agent technology.



PRISMS SUPPORT NATIVE CLOUD INFRASTRUCTURE CAPABILITIES LIKE AZURE'S VTAP CAPABILITY.

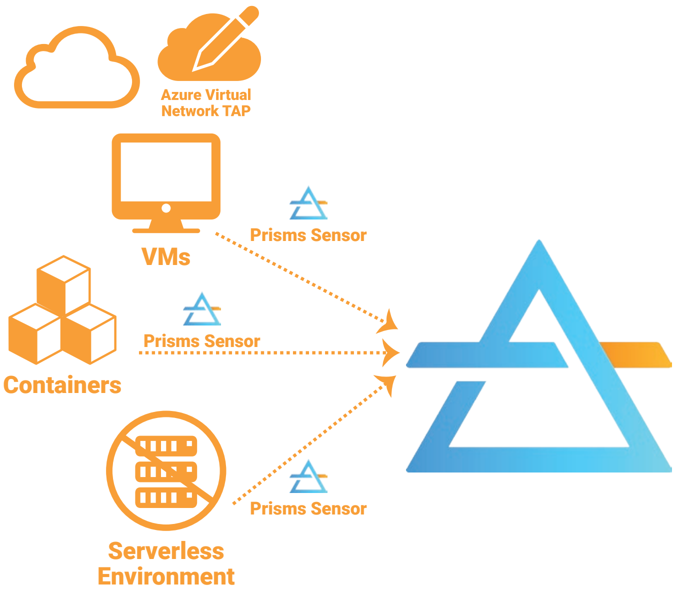


NUBEVA PRISMS FILTERS, ENHANCES AND PROCESSES PACKET TRAFFIC TO EXACTLY MATCH THE IDEAL INPUTS FOR YOUR TOOLS, TEAMS AND PROCESSES.

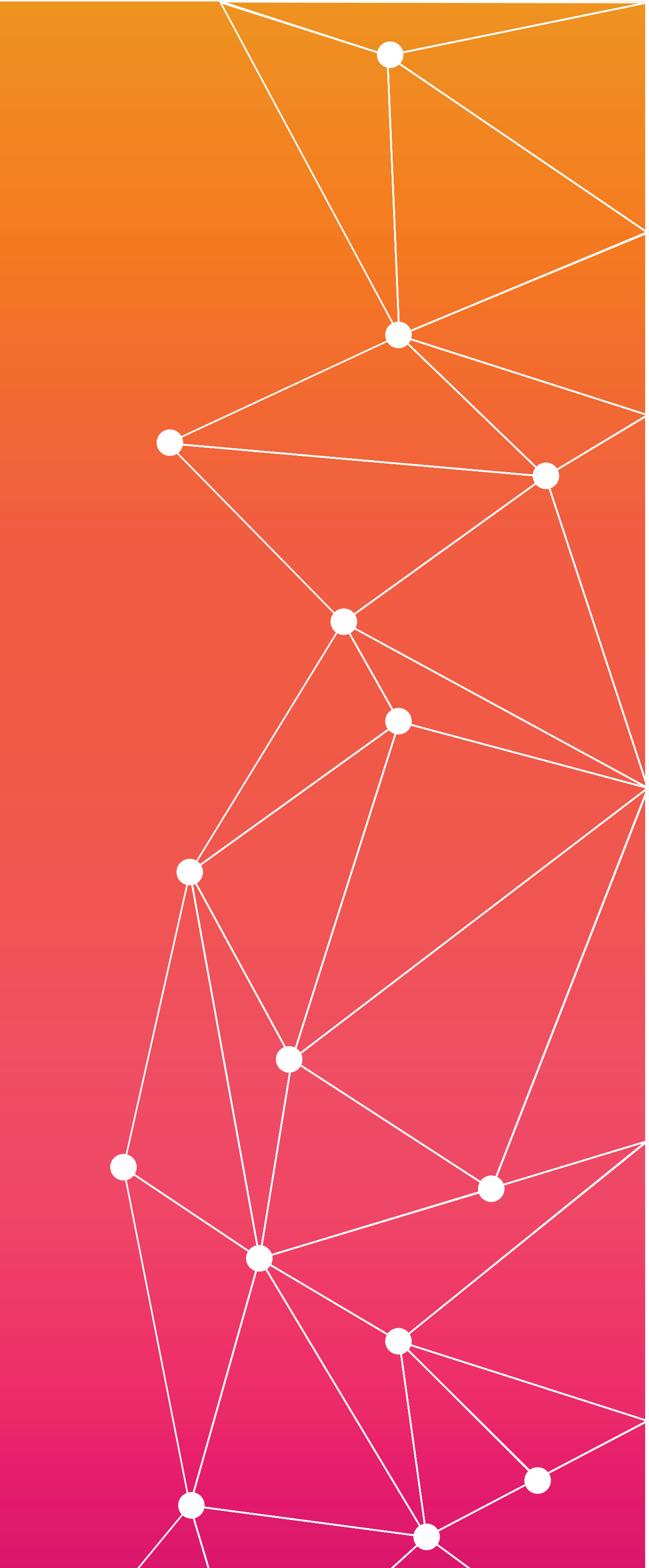
The Prisms sensor is built from a docker container model rather than a driver-model.

As a result, Prisms:

- Performs more effectively
- Provides a smaller footprint
- Is more tightly contained
- Is easier to manage
- Is self-updating and self-dissolving
- is completely secure



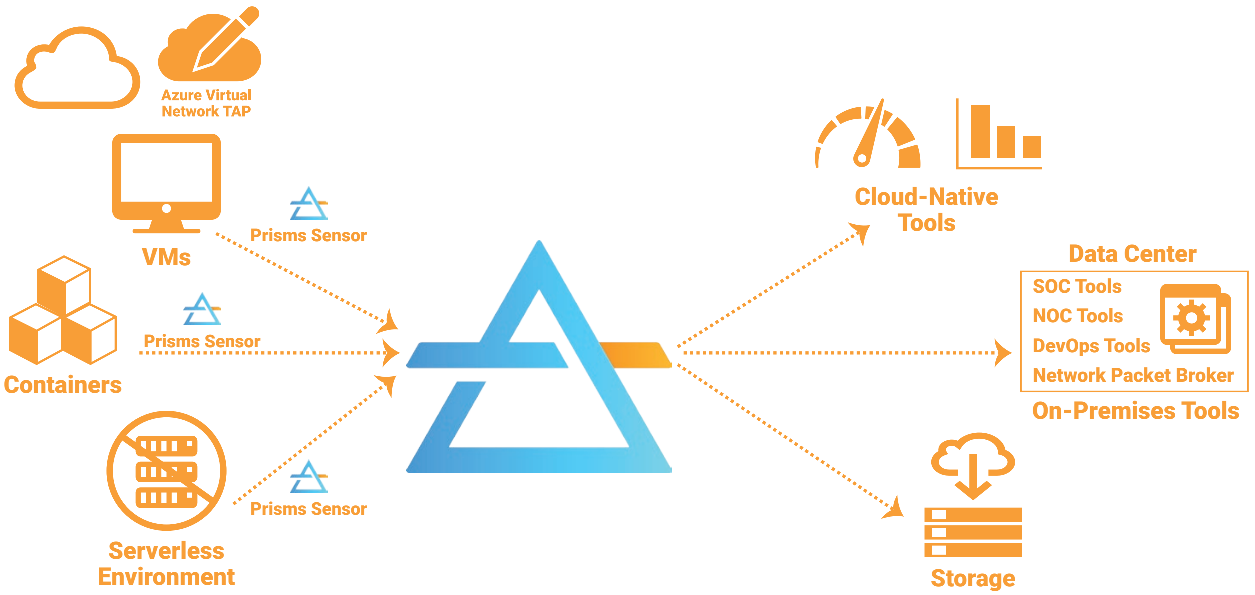
The second part of the Nubeva solution is the Prisms Service Processor. This is a packet processing engine that ingests raw packet capture from any number of sources – whether those sources are VTAPs or Prisms Sensors or something else. Then the Prisms Service Processor aggregates that traffic, filters that traffic and enhances that traffic so that it is perfectly matched to the needs of the applications, tools and destinations where it will be sent.

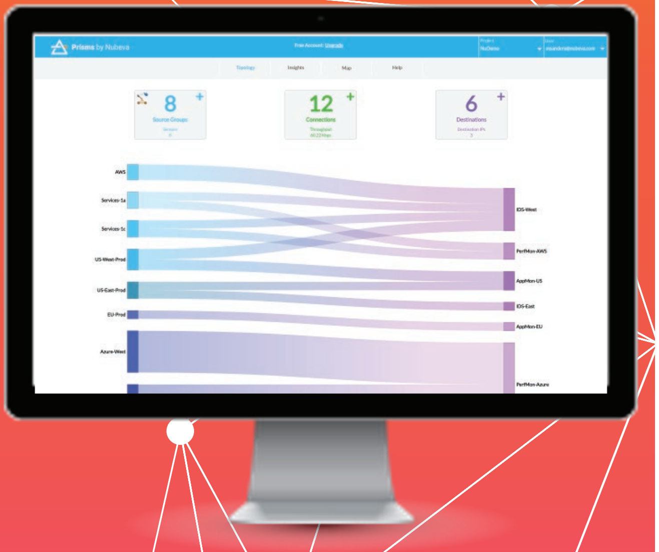


NUBEVA PRISMS REPLICATES THE PROCESSED PACKET TRAFFIC TO ANY NUMBER OF DESTINATIONS.

Finally, the Prisms Service Processor replicates the traffic out to where it is needed. It can replicate the processed traffic to in-cloud native tools, in cloud storage, or ultimately to your tools, teams and processes in your very own data center. It can send the processed traffic over DirectConnect or ExpressRoute.

This is why capabilities like filtering and processing become very important. Nubeva Prisms filter packet traffic, delivering the packets needed by your at-home tools. This cuts down on data transit charges and it helps your tools and teams run more efficiently.



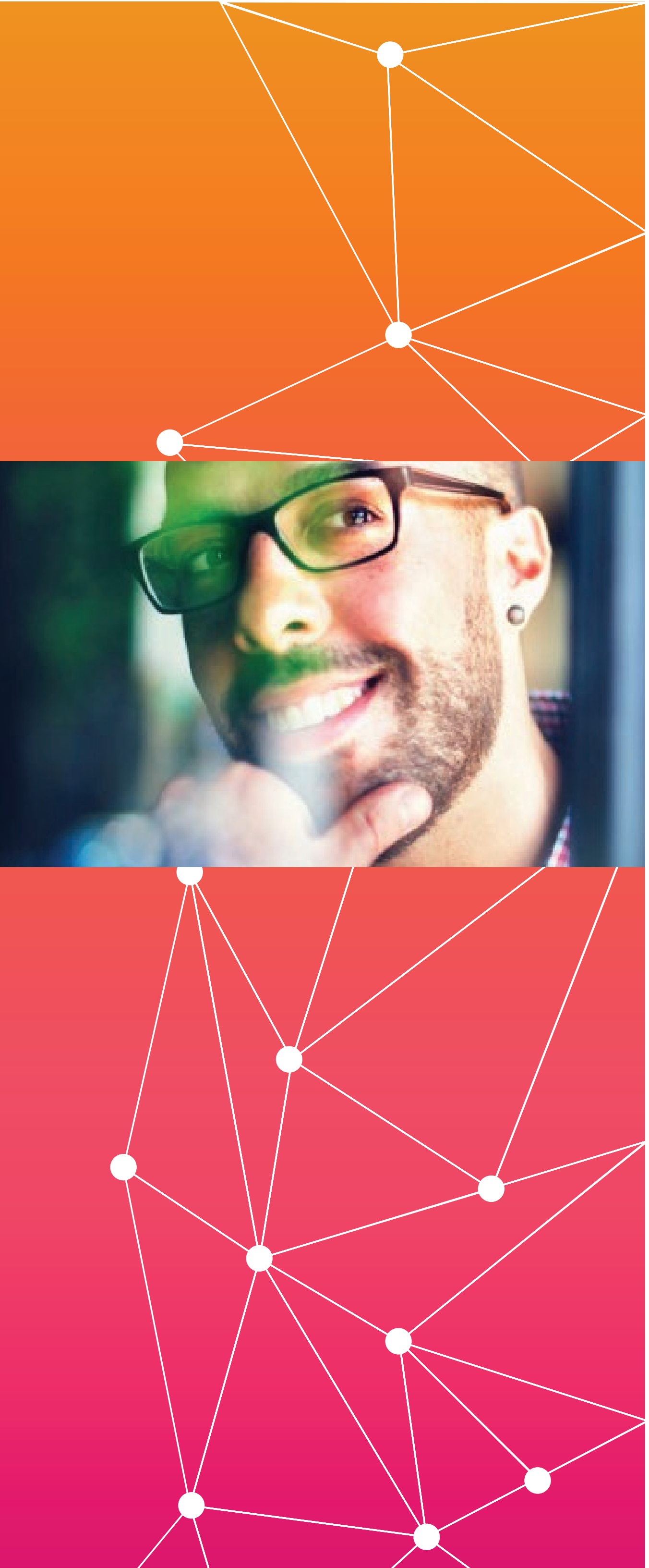


NUBEVA PRISMS IS DESIGNED FOR DRAG-AND-DROP SIMPLICITY WITH DEEP SOPHISTICATION.

The Prisms Service Processor itself is built on next-generation, cloud-native technology. It is built on an elastic container technology that is infinitely salable and very low cost. It eliminates the costs and headaches of spinning up and managing VMs to process the traffic.

This is all managed by a very powerful yet simple, drag-and-drop easy user interface. It is rules- and policy-based instead of hard-coded and fixed. In the cloud, you cannot expect to have hardened configurations and still have all your scenarios covered. You need rules and policies that can flex with elastic compute environments. Nubeva Prisms helps you create these kinds of flexible rules so that you can write policies that, for instance, say, “everything with the word “database” in its description should send packet traffic, filtered like so, to this inspection tool.” As resources come and go, the only way to truly manage an environment like that is with automated rules and policies.

THIS IS ALL MANAGED BY A VERY POWERFUL YET SIMPLE, DRAG-AND-DROP EASY USER INTERFACE.



INNOVATIVE SPLIT-SaaS ARCHITECTURE DELIVERS SaaS CONVENIENCE AND ENTERPRISE SECURITY.

Nubeva Prisms is delivered via a powerful Split-SaaS delivery architecture. The management system itself resides in a shared SaaS model. This way, you get the benefits of instant-on operation, not having to manage the software and lower operational costs. All the data and the entire data-control plane stays within your cloud subscription. We do not ask for or store credentials. The system does not reach into your account, it only responds to REST calls that originate within your environment. Ultimately it delivers the integrity and security of an enterprise class solution but with the convenience and simplicity of SaaS. This is an extremely powerful approach and a new way in thinking about security the public cloud.

At the end of it all, it means that you gain full capability to acquire, process and distribute all the packet level traffic from your public cloud to your security and monitoring teams and tools.

54%

of organizations have no visibility into how — or if — data management policies are applied and enforced.

Source: 2018: State of Virtualization in the Cloud by Druva

The Nubeva Difference

THE SIX KEY ADVANTAGES OF NUBEVA PRISMS.

1

See More Packet Traffic.

Nubeva Prisms can see more traffic from more sources. We have the simplest, easiest ways to see and acquire traffic. From our support for Cloud-supplied infrastructure like VTAPs to our next-generation sensing technology that spans Windows and Linux VMs to container services and beyond. It is designed to be as modern and elastic as the cloud, we simply see more in the cloud because we were built for the cloud.

2

More Powerful Packet Processing.

Nubeva Prisms has a better packet processing model. This very light and powerful way of acquiring traffic and then send it to an elastic, containerized processing engine – whether it be one in your subscription or one in every VPC or VNET – it is flexible in its deployment and provides more advanced packet processing options.

3

More Flexible Distribution.

Rather than restricting where you can send traffic or having heavy requirements – like agents required on the destination targets – we can send traffic anywhere. Whether it be a load balancer, an endpoint tool, a cluster of tools that we balance against or an in-cloud or out-of-cloud destination, we support any kind of targeting that you need.

> **Protection layers [provide] the capability to monitor application behavior and ban suspicious activity; prevent exploits by using the latest threat intelligence; and find and automatically patch vulnerabilities, to safeguard data and workloads moving across cloud infrastructure, from threats.”**
>
> *Maxim Frolov, Vice President of Global Sales, Kaspersky Lab*

4

Superior Ease of Use.

Nubeva Prisms delivers superior ease of use. Ultimately, the automated approach and rules and policy-based approach means that it becomes a fire-and-forget solution. Nubeva prisms can integrate with and be automated by any other system. This is not yet-another-cloud-platform. Set your rules, direct your traffic and get back to work with the tools, teams and processes that you rely upon to keep your business running.

5

Massively Scalable.

Nubeva Prisms is massively scalable and fully redundant and resilient because it's designed for the cloud. It has been tested with hundreds of thousands of source inputs that can be monitored and hundreds of Gigabits of traffic.

6

Modern, Innovative Architecture.

Nubeva Prisms has a superior architecture with SaaS benefits and ease combined with enterprise-grade security. The Split-SaaS architecture is superior to old legacy approaches. It has all advantages of convenient SaaS and all of the security of an enterprise control system.

PRICING.

At Nubeva, we believe that pricing should never be a barrier to security or cloud adoption. That's why we're disrupting the industry with our extreme affordability.

Disruptive pricing is built into our DNA. We believe that the fabric costing more than the tools is backwards. So we're flipping the model. No longer will the tires be more expensive than the car. Nubeva believes that everything in the Public cloud should be instrumented. So we've made it so that cost will never get in the way.

WE'RE DISRUPTING THE INDUSTRY WITH OUR EXTREME AFFORDABILITY.

ABOUT NUBEVA

Our mission is to deliver simple, easy to use and affordable software that enables enterprises to run their trusted application, network and security monitoring in public clouds without compromise.

How? *Cloud Style.* Cloud is speed. Cloud is easy to use. Cloud is easy to implement. The cloud is about transforming complex IT into simple services. The cloud is made up of plug and play systems and subsystems that can be integrated to form even greater solutions. The cloud fosters collaboration and reduces cost.

Nubeva was born in the cloud for the cloud. Our tools are rapidly evolving. Our goal is to make it better, faster and more affordable. Nubeva Prisms is ultra-secure and priced disruptively low because to achieve our vision – we believe cost shouldn't be a barrier to security, accessibility, visibility and productivity.

**To learn more or request a demo,
visit nubeva.com or call 844.538.4638**