NS1 Labs

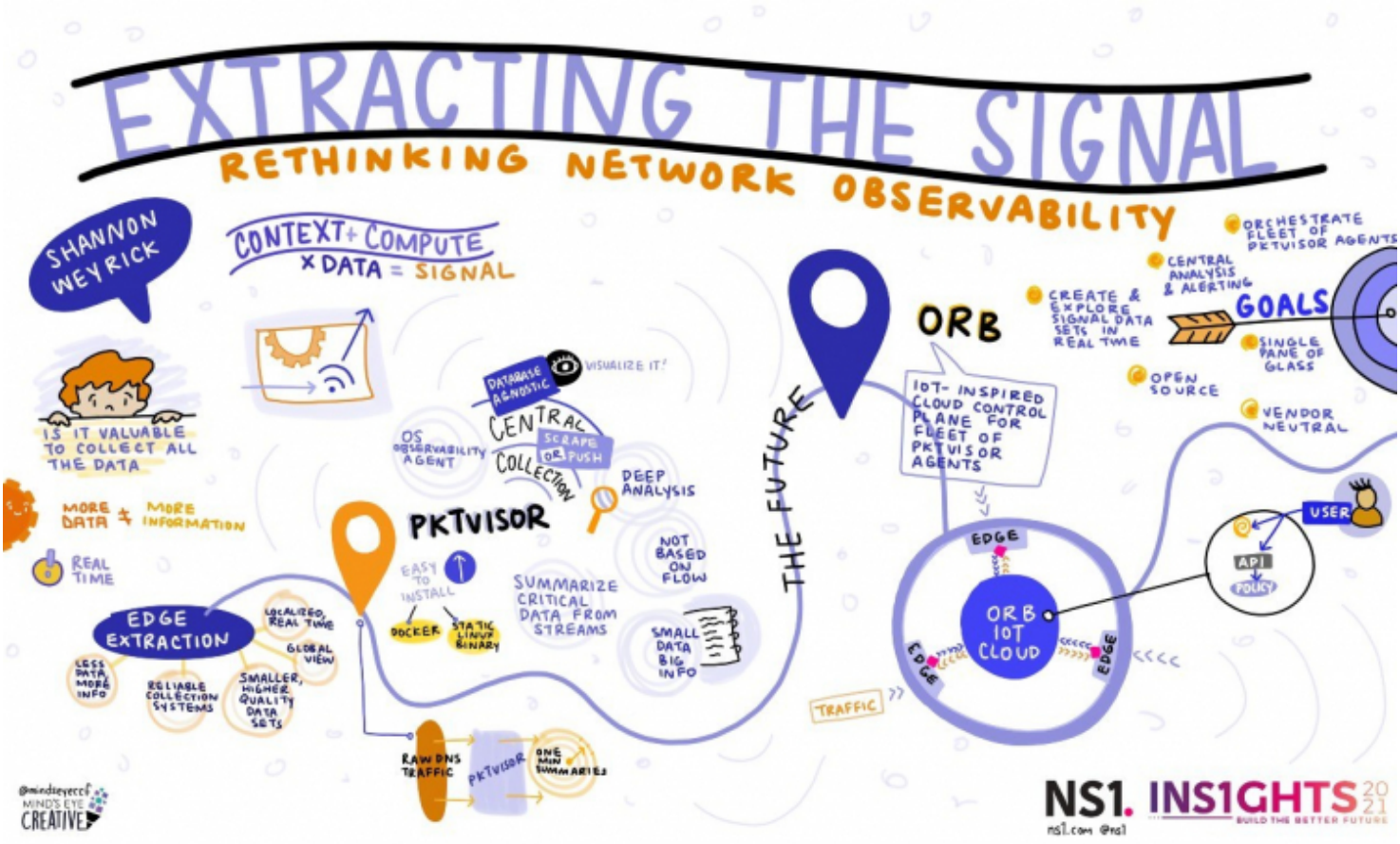
Extracting the Signal: Rethinking Network Observability

Posted by
Shannon Weyrick on
July 21, 2021

The concept of observability has come a long way. We have a lot of great tools, platforms, and technologies for collecting metrics from across our tech stacks, including applications, VMs, containers, clouds (public and private), networks, and beyond. We have the right frameworks, SDKs, SaaS products, agents, and giant cloud data warehouses to help us collect data of every dimension.

But more data does not necessarily mean more information. Data is just bits on a wire until we take it and turn it into actionable information; or in other words, we need to extract the information from the data for it to be truly valuable. Data that is collected but never turned into information is expensive and wasteful of resources, slowing our observability pipelines and dashboards and even potentially making it harder to gain actionable insight as we struggle to find what's relevant and how to interpret it.

At NS1, we regularly think about extracting actionable information from network data streams. After all, when you're operating mission-critical, globally distributed services like we do, it's incredibly important to understand exactly what is happening across the network in real time - for general operations and traffic engineering but especially during a DDoS attack, for example. However, the traditional tools for network observability can get swamped with too much inactionable data, and miss the needles in the haystack that you really need to understand to address network and traffic issues.

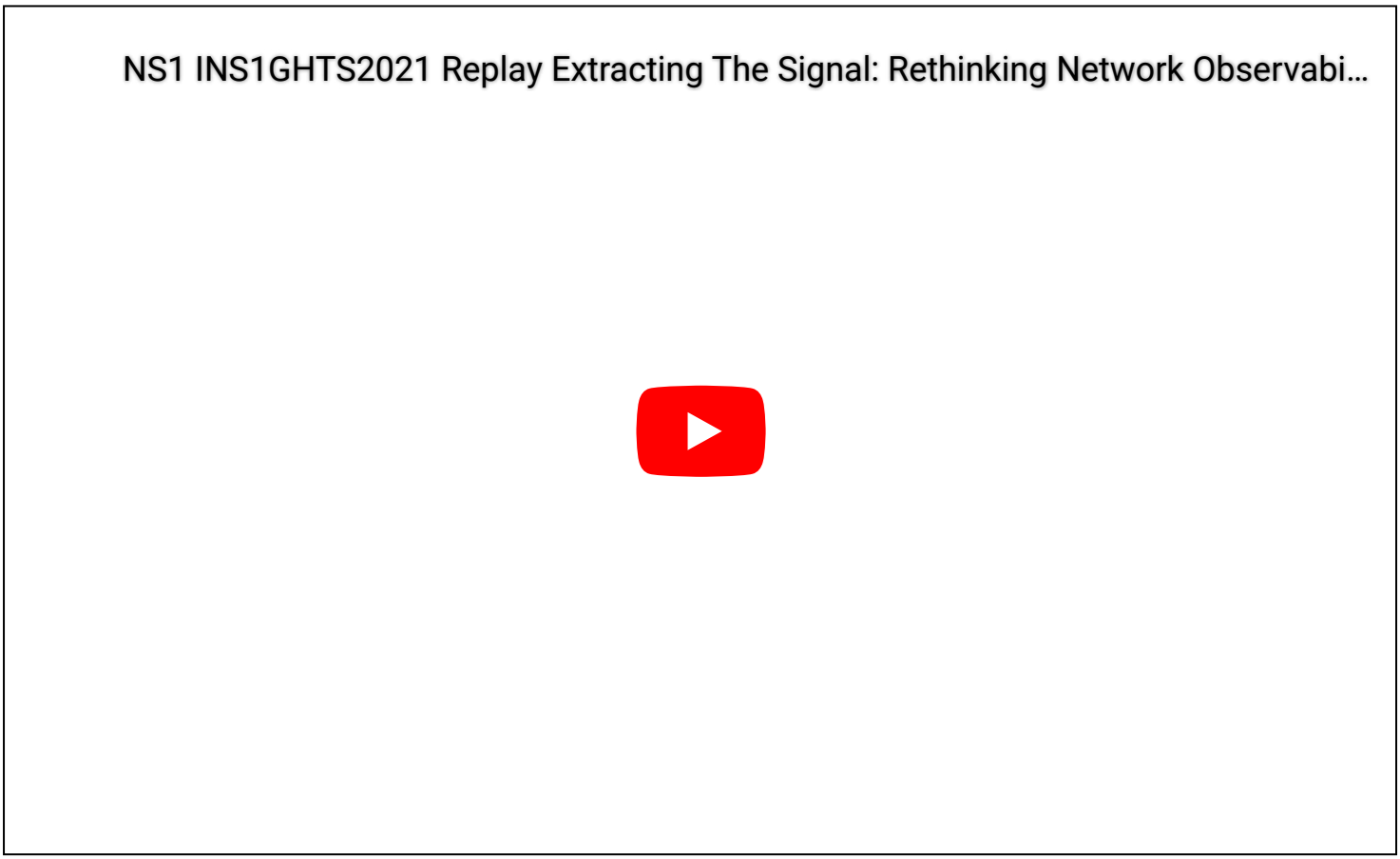


That's why **NS1 Labs** is building open source observability and business intelligence tools like **pktvisor** and **Orb**. Keep reading for a quick overview of what pktvisor and Orb are solving for, or watch my full session from **INSIGHTS2021: Build the Better Future** below for a deeper dive.

Watch the Full Session from INS1GHTS2021: Build the Better Future

Watch my full session from INS1GHTS2021 for an in-depth look at how pktvisor works, and our current progress on Orb.

You can also view all the replays from INS1GHTS2021 in our **replay hub**.



Pktvisor - a Dynamic Edge Observability Agent

To extract the signal within our data, we need the following:

- The raw data streams to analyze
- A domain specific understanding of what we're looking for (what data is actually valuable?)
- Compute power to pull the appropriate information out of the stream

Then we need to make a choice: where do we apply the compute power? Do we collect all of the raw data streams to a central location and then apply the compute in batch, or can we instead push that out to the edge, colocated with the source?

pktvisor is our open source observability agent that pushes the extraction process to the edge. It's a production ready piece of software developed over years of operations at NS1, **available today on GitHub**. It is designed to be installed at your edge where it can tap into data streams at the source - for example, via packet capture, DNSTAP streams, and potentially other streams in the future. With pktvisor, you can extract business intelligence that's passing by in these streams in real time, and get both a local and a global view of the information that it's able to extract. pktvisor uses streaming algorithms to do deep analysis of these data streams in real time.

How pktvisor Works

Since pktvisor has its origins observing critical DNS traffic, let's imagine the querying process of DNS for a moment. If pktvisor is tapped into this stream of packets that are flying by, it's decoding and analyzing DNS packets as they go by on the wire (and it really decodes all of these streams; it's not based on sampling technology like sFlow or NetFlow). There's information in there we really want to get to like IP addresses, ports, query IDs, the DNS question that's being asked, among other things. As this raw traffic comes into the pktvisor system, sometimes it will be at a high rate, sometimes it will be at a low rate.

pktvisor's job is to create uniform-sized, one-minute summaries of that traffic - this is the extracted information that we have pulled from the raw data. The uniform size is a key property that helps you avoid placing downstream pressure on your observability systems

when facing unusual traffic spikes (i.e., during a DDoS attack).

Because the goal is to have the highest information to data ratio that we can, and to keep the size of the summaries small, pktvisor only collects the information we care about. In the context of DNS, this means top queries, query types, result codes, IP sources, and so on (**a full list is here**). This is what we mean by “extracting the signal” - rather than sending large batches of raw data back to a centralized source, we’ve pushed the compute to the edge. Only after we’ve extracted the information do we collect it to a central location for dashboarding and further analysis and alerting.

Where Orb Comes In

The goal with **Orb**, a new open source project in the works from **NS1 Labs**, is to create a control plane that dynamically manages a fleet of pktvisor agents and collects the results. To do this, we're using IoT technology to connect and control these fleets in real time.

With Orb, we add critical functionality beyond just collecting the extracted information centrally: we connect the edge agents into a centralized control plane which is able to communicate with the agents and to give them instructions. The idea is to be able to run an agent on edge locations as close to your data streams as possible. These edge agents will then connect into the control plane using IoT technology, allowing you to reprogram agents dynamically in real-time.

With Orb and pktvisor, we will make Dynamic Edge Observability a reality. Pktvisor is open sourced and available today. Orb will be released - fully open source - later this year.

Here’s how you can get engaged with Orb:

- **Sign up to get updates on Orb and pktvisor from the team**
- Check out **Pktvisor’s docs** and get started with the ready-made docker image or other options
- Star **Orb** and **pktvisor** on Github and contribute, open issues, or read the code
- Bookmark **GetOrb.io** for future releases
- Join the **NS1 Labs Slack** to engage with Shannon and the rest of the Orb community

Learn more about NS1 Labs in our recent blog post: **A Wave of Open Source Innovation at NS1 Labs with Orb and NetBox**.

Further Reading

FEATURED

Orb - A New Paradigm for Dynamic Edge Observability

Last week we announced the launch of NS1 Labs - learn more about Orb and pktvisor, two open source technologies developed by NS1 Labs that align with our vision for the future of application and audience connectivity.

Read the Article ⊙

✳ View all Resources

NS1.
an IBM Company

ABOUT

Blog

News

Careers

Diversity & Inclusion

SUPPORT

Help Center

NS1 Status

Documentation

Contact Support

SUBSCRIBE

Email Address

Subscribe

Partner Portal

Terms of Service

Privacy Policy

Responsible Disclosure Policy