JASK

DATA SHEET

DPI: Data for the SOC

Traditionally, to gain end-to-end visibility within an organization, the choices for security teams were limited.

OPTION 1

Netflow, which meant enabling all routers and switches to send data from the distributed network into a central location. This process could be (and often was) automated in larger organizations, but then the question became, "what to do with all this data?"

Perhaps the most logical choice for most was to send the information to your SIEM as this data is useful in understanding connections, network peers and data flow rates/volumes. For a true security use case, however, netflow can fall short in terms of providing the context required to make informed decisions, and the volume would either crash your SIEM or your budget.

Beginning with the data, netflow provides the basics such as source, destination, ports and bytes transferred, ultimately providing no insight to what is happening within the connections. Do the ports align with the protocol used? Is the traffic encrypted when it should be in the clear? Is the higher-level protocol carried by this connection behaving normally? These are just some of the questions that cannot be answered with netflow alone.

As for the budgeting aspect, SIEM's and even netflow-specific tools are largely based on throughput charging or a consumption tax on either gigabytes per day or events per second (EPS), meaning netflow monitoring for the entire enterprise was cost prohibitive. In addition, these systems were deployed in an on-premises appliance/server model, increasing the footprint of the datacenter and leading to higher operations and management costs to keep them up to date and running.

OPTION 2

Packet Capture, which suffers from the same constraints of time and money requiring advanced resources to derive value, massive amounts of licensing and hardware, and short retention windows.

While packet capture provides DVR-like capabilities to the network traffic, its cumbersome and costly nature is too prohibitive and constrained to the perimeter. This requires massive amounts of hardware to collect and store the data, which in turn drives up operational costs for customers. In addition, even with the storage capabilities in place, throughput-based licensing and limited

retention times reduce the value the solution provides. Piling on, there is the lack of industry professionals to interpret the data. It is well-known that even junior level security talent is hard to find and demands a premium; even so, finding analysts that can make use of packet capture is an insurmountable challenge.

ANSWER // JASK

At JASK, we've found the sweet spot is deep packet inspection (DPI), which falls somewhere in the middle, providing the best of both without the limitations.

The data provided by the network sensor is much more robust than netflow. JASK utilizes DPI on a protocol level. Currently JASK analyzes over 20 different protocols including some encrypted protocols. The DPI analysis allows far more insight to the network conversation then netflow. For example, we see UA strings in HTTP connections, TLS versions and keyboard attributes in RDP sessions.

Similar to packet capture solutions, JASK uses network sensors to analyze traffic off the wire providing the full context of the network activity. This is done with a tap or span port or via a feed from a packet broker technology such as Gigamon.

The difference, however, is that JASK's solution utilizes a lightweight software deployment model, and while you get 99 percent of the context as you would from full PCAP, for your security investigations the metadata extracted only amounts to roughly 2-5 percent of overall traffic volumes providing massive cost savings in both processing and storage.

This allows network sensors to be deployed anywhere throughout the enterprise and is not limited only to perimeter deployments or locations with large data centers to house the equipment. JASK does not charge per sensor or by throughput so customers are able to obtain the detailed visibility into their network that was previously out of reach.

JASK network sensor provides full layer 3-7 visibility from the perimeter to the core, and even in remote sites or branch offices providing end-to-end visibility to uncover blind spots. In combination with an entirely SaaS-based deployment model developed on the latest in big data technologies, the JASK ASOC platform allows for a lightweight, cost effective deployment, and horizontal scale not available in the previous generation of technologies.

The number one question received about the true ability for DPI to replace PCAP from enthusiasts is as follows: "What about the payload?" The concern is that sometimes a file download was observed that could be hostile. SOC's with advanced forensic capabilities will want a copy of the file for sandbox analysis, etc. Yet in reality, this is not a problem. JASK's DPI technology allows for file carving, which selectively extracts payloads that may be useful for later investigation.

As an open platform, JASK allows customers to tune models, apply their own queries to their data unlike the latest wave of black box analytics tools. Combining threat intelligence, traditional patterns/signatures, and the latest in non-signature based machine learning to a rich DPI dataset, JASK's neural network helps in the detection of modern threats and provides the insights you'll need to triage security incidents with conclusive answers and next steps while consolidating multiple point solutions.

If the use case is to get data from the network and determine who is "talking" to whom, netflow alone may suffice. If you have unlimited funds, storage, and an elite analyst team who can read binary PCAP, perhaps recording every byte is your cup of tea. However, if you want to overcome the barriers of traditional technologies, provide the detailed visibility with context required for security investigations while remaining cost-effective and efficient in your security investments then try JASK. You may just true hidden value.