Contextual Information - The ABCs of Network Visibility

Contextual information is data that gives context to a person, entity or event. In other words, context-awareness is the ability to extract knowledge from or apply knowledge to information. Let's take an example. As you finish up watching a movie or show on Netflix, you are served with similar content or the next in the series. You like that as it caters to your interests. Netflix uses context aware technology to improve user experience by extracting contextual metadata. Similarly, the Four Seasons hotel chain is well-known for its legendary customer service, which includes staff addressing each guest by name. How do they do this? They use context-awareness.

What is Context Awareness for Data Networks?

In today's digital world, what lays the groundwork for context information are environmental factors, data discovery and aspects that exist in the IT stack. These include devices, users, data classification, networks, URLs, the applications in use, potential threats, and even considerations affecting the value of business data. And of course time and location. A few easy examples are Google Maps (or Waze) that follow your travels, calendar notifications of your upcoming appointments, app preferences, and accurate contact selection when you enter only a few letters. This is known as "contextual awareness," where a given computing device uses user-specific data, like location-based technology and sensors to determine their circumstances. It seems as if the device "knows" where you are and what you need. The combination of information, along with correlated knowledge, is what makes its context-aware data processing so powerful.

Typical Use Cases

Why is context aware data so important in today's world? Context-aware data processing allows you to optimize the inspection, analysis, and recording of the data used by your security and monitoring tools within your network.

Improve network security – The emergence of widespread threat actors and organized cyber-criminal organizations have created an environment where companies are under constant siege. An effective tactic known as application intelligence using context-aware security analytics has become one of the central pillars for threat detection and prevention. Some security tools like an intrusion detection system (IDS) look at session and application layer data, trying to find pattern matches against a database of threat signatures. But, not every tool is designed for every traffic flow. Before distributing network traffic to your tools, context-aware data processing applies its intelligence to network traffic flows to intelligently distribute only relevant data to security and monitoring tools. For example, this means email monitoring tools will get email traffic only.

Better insight into application traffic - Understanding the context of users, devices, and locations, provides important context for applications. It is about filtering traffic by geography and removing duplicate packets before it reaches a monitoring tool. For instance, a gaming company that serves up games through a social media channel, could identify the city, devices, browsers and applications that were causing a performance issue with a context-aware application intelligence tool and rectify the precise problem. Performing additional functions like this can be critical to network security monitoring, but it all starts with application intelligence.

Better insight into network traffic - To get the most out of your monitoring tools, the data will typically need to have some sort of contextual data processing applied. This means the addition (or removal) of VLAN and port tags, removal of duplicate packets, addition of time stamps, header stripping, packet slicing, etc. may need to be applied to the packet data so that it is optimized before being passed on to the monitoring tool for analysis. This "preconditioning" makes the monitoring tools more efficient and improves time to resolution.

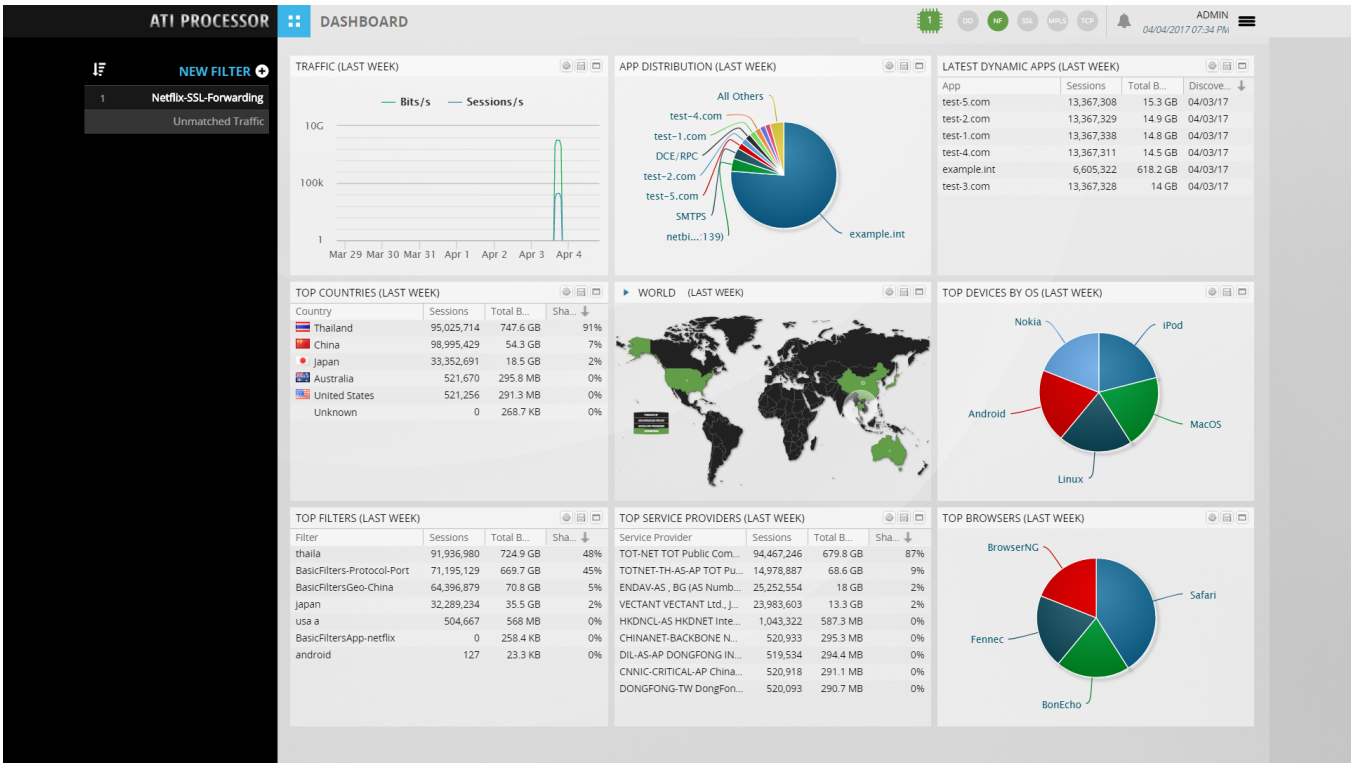
Considerations

The following are some things to keep in mind:

- Make sure your visibility is easy to use but has all the functionality that is needed – For instance, to harness real application intelligence, it needs to support hundreds of application signatures built-in, as well as have a service feed to add new ones and keep everything up to date. You also need to be able to easily filter based upon those application signatures. A dashboard that displays statistics, so you can see what applications are generating traffic, the amount of traffic, and the number of sessions contributing to the traffic volume is also required.
- Have a plan to use the information - One benefit of context-aware data processing and analytics is that it can identify attackers based upon their activity and behavior on your network. For example, last year's massive breach at Sony Pictures may have been preventable if security personnel had the capability to identify abnormal and large-scale data transfers. However, you must have technology and processes in place to capitalize on the information so that you can get the maximum benefit of it.
- Be sure your network visibility solution can scale – As data grows exponentially, it is stored on an endless number of devices and in the cloud, is accessed by employees, partners, and customers via connections from just about everywhere, you can imagine the wide scope of the contextual data. A dynamic, intelligent and robust solution is required for monitoring the events and avoiding the security threats.

More Information on Context-Data Awareness

The Ixia Security Fabric™ is a powerful network visibility engine and its context-aware data processing engine provides administrators with a dashboard of graphs, charts, maps, and statistics of known and unknown applications, geographies, and devices on their network. The engine can also act, by forwarding traffic to specific tools based on contextual details and generating enhanced NetFlow data, such as country, region, browser, operating system, and application name. This engine also provides you with control of data conditioning functions (like deduplication, timestamping and burst protection) to achieve reliability and efficiency in your network of security and monitoring tools.



For more information visit https://www.ixiacom.com/solutions/network-visibility.