

The Startup Observer

<https://startupobserver.com/smart-data-is-the-first-step-to-smart-analytics/>

Smart data is the first step to smart analytics

24/05/18

By

Ayushman Baruah

-

May 24, 2018



One of the biggest problems IT faces is the large volume of unstructured data delivered at high velocity from a variety of disparate sources. This “random” data does not translate into actionable insight, even when used with advanced analytics. In short, business analytics that rely on a dataset that has not been normalised and correlated in the context of service delivery, operations, and business performance, will simply not be effective. The bottom line is that the quality of business insight is contingent upon the use smart data.

Clearly, analytics without the right data means nothing. And, that’s where smart data comes into action. US-based smart data solutions company,

[NetScout Systems](#) claims to solve this challenge by offering smart data that helps in getting the right data, fast, to the people and systems that need it. “We distill real time, precise intelligence from the noise of traffic data, simplifying the complex without losing the details,” the company said at the NetEvents Global Press & Analyst Summit in San Jose.

NetScout’s smart data technologies include Adaptive Service Intelligence (ASI) and Active Threat Level Analysis System (ATLAS) that collectively claim to have the visibility and insight into more than one third of the internet and global enterprise and subscriber traffic.

Netscout’s patented Adaptive Service Intelligence (ASI) technology generates smart data based on software-centric pervasive instrumentation of traffic-flows that are collected and processed at the source – from physical and virtual (SDN/NFV) infrastructure on-premises, software-defined data centres (SDDC), and hybrid cloud environments – to produce service contextual metadata in real time. This allows you to enhance/infuse your big data analytics projects with smart data that can offer critical insights into service delivery, business operations, and other vital business performance indicators.

Active Threat Level Analysis System (ATLAS) is a global collaborative platform with more than 300 Arbor service provider customers sharing traffic and threat data, giving Arbor visibility into approximately one-third of all Internet traffic. (Arbor Networks Inc., the security division of Netscout). Arbor’s Security Engineering & Response Team (ASERT) utilizes a combination of ATLAS information, in-depth malware research and data from real-time botnet activity monitoring to understand current threats. ASERT knows when an attack is launched immediately, and what data the attackers are receiving back, enabling Arbor to provide much needed risk context. Through this unique global lens, Arbor allows defenders to move at the same speed as the attackers regardless of where and whom they are targeting.

When Smart Data Meets Superior Analytics

The Netscout nGeniusONE service assurance platform offers superior analytics of the smart data generated by ASI. It performs contextual analysis of the smart data and visualization of complex and geographically dispersed service delivery environments. The most challenging aspect of this analysis is to identify the inter-dependencies across the entire service stack, including applications, networks, compute, service enablers and databases, end-to-end across on-premises and cloud environments.

To accomplish this task, the nGeniusONE platform analyses smart data generated based on monitoring traffic flows across a large number of physical and virtual interfaces, servers, transactions, applications, protocols, devices, and users. The analysis is then converted into actionable insight with top-down service oriented workflows that guide the user through the triage process of root-cause analysis. With as few as three clicks of a mouse in nGeniusONE, the user can navigate in context from the service dashboard that offers visibility into critical service issues, to the service monitor, that provides the details on load, latency and errors, to the hop-by-hop session analysis. Deep dive packet analysis is optional and used for more complex investigations and forensics analysis.

NetScout has customers in more than 120 countries across the globe including 90% of the Fortune 100 companies. It is publicly traded in the NASDAQ and has 3000+ employees.