

AnubisNetworks deploys real-time capabilities to tackle 'big data' threat intelligence

Analyst: Javvad Malik

17 Jun, 2013

The 'big data' security problem has been around for a number of years, and in that time, many vendors have attempted to address it with varying degrees of success. Some of the most common challenges in processing big-data security events have to do with the scope of data and the speed in which it can be processed. AnubisNetworks believes its Streamforce product can provide the answer to these challenges with its capability to consume data from both inside and outside an enterprise and undertake analysis in real time.

The 451 Take

AnubisNetworks has an interesting take on the big-data security problem, which we see as a positive. However, the company may find itself battling traditional SIEM messaging and positioning to get a seat at the table. Despite this, what we like about the company is that it has built out its capabilities by remaining true to its core skill set and can position itself as a partner not just to SIEM companies but a multitude of vendors. Once it has time to establish its Streamforce offering, we wouldn't be surprised to see a large infrastructure company show an interest in acquiring it.

Context

Porto, Portugal-based AnubisNetworks was founded in 2006 by Francisco Fonseca, CEO, Nuno Silva, COO, and João Gouveia, CTO. The company started in the email security space providing managed

services and, subsequently, cloud-based security services that were sold primarily to telcos, service providers and large corporations. It also developed consumer products such as MyFamily. Leveraging the experience gained from these deployments, Anubis developed its real-time threat-intelligence product, StreamForce, which it launched in April.

The company currently employs about 25 people across offices in Portugal, London and Jakarta – with a view to set up an additional office in Brazil. Anubis says that it has received a lot of interest from these regions, and its current strategy is to focus primarily on selling to Southeast Asia and South America, where competition is comparatively less.

There are roughly 20 ongoing trials for the threat-intelligence offering, with a lot of interest generated from large telcos, financial institutions and governmental departments. The company doesn't have a large direct sales force and is actively seeking technology partners.

Products

Streamforce is AnubisNetworks' real-time threat-intelligence platform that processes, analyzes and correlates events from multiple sources. On the surface, its event-correlation capabilities make it appear similar to a SIEM product, but AnubisNetworks has developed Streamforce in a slightly different way. The product does not utilize a database to store data in order to provide real-time capabilities. Rather, it performs correlation on the fly and as close to the source as possible. This allows a constant stream of intelligence to be produced from big-data sources that would be very difficult to achieve at speed with a database-dependent SIEM product.

The Streamforce platform consists of sensors that collect events from sources in real time. The feeds can be internal to a company – i.e., private, such as email, Web, DNS feeds, etc. – or the platform can utilize publicly available data as feeds, such as site reputation, honeypots, sinkholes, Twitter and so on. AnubisNetworks can also leverage its own existing sources of information, such as Mailspike, to provide IP reputation feeds. The architecture is distributed and designed to be scalable so that multiple feeds coming in can be processed simultaneously in real time.

Owners of private feeds can specify where the data can be shared. For example, a vehicle-tracking company publishing feeds relating to the location of its vehicles may only allow its data to be seen by its customers or by law enforcement. Subscribers have the ability to run queries against the platform to manage and design processes, queries, feeds and desired output. Anubis says that this can allow customers to filter out unnecessary data and send only relevant information to the SIEM product for storage and analysis.

In addition to having the ability to run queries, 'applications' can be built utilizing the Streamforce API. One such application that Anubis has developed as a service is Cyberfeed. Cyberfeed takes inputs from security-specific sources, both internal to Anubis and from industry sources. The information is correlated and made available to subscribers with a management dashboard and visualization UI to present data on real-time botnet information, fraudulent websites, spam-sending systems, and so on. Cyberfeed is available to customers on a yearly subscription basis.

Competition

One could easily see AnubisNetworks competing in the crowded SIEM sector with vendors like HP (ArcSight), IBM (Q1 Labs), RSA (envision), LogLogic, McAfee (NitroSecurity), Alert Logic, LogRhythm, SenSage, Red Lambda, AlienVault, Splunk and the like. However, Anubis will likely point to the differences in architecture as making it more complementary to a SIEM product by providing pre-filtering across much larger external data sources. From a Cyberfeed perspective, Anubis could find itself competing with any vendor that provides external threat feeds, such as Arbor Networks, Seculert, Mandiant, Lookingglass Cyber Solutions, etc.

It will be interesting to see how Streamforce will fit into the anti-malware ecosystem. On one hand, we can see it being a good fit to provide early intelligence to a vendor like Trend Micro, Sophos, McAfee, Microsoft, Kaspersky Lab, F-Secure, BitDefender and the like - but at the same time, its malware-detection capabilities could put it in competition with these companies.

SWOT Analysis

Strengths

The distributed architecture, real-time capabilities and ability to process large data feeds that can be interrogated and visualized in a UI provide insights that will be difficult to ignore.

Opportunities

Anubis will initially need to get some satisfied paying customers to prove it's a viable security product. Once established, the opportunities are plentiful. We could see technology vendors wanting to partner or OEM its offering. Also, a large infrastructure company like IBM, HP or McAfee may be interested in wielding AnubisNetworks' technology under its own banner, so the company will need to keep the idea of an exit by way of acquisition as a real possibility for the future.

Weaknesses

The company is still in its early stages, and some potential customers may not be able to grasp the capabilities or relevance of the product. If AnubisNetworks could leverage public sources of information to create more applications, that would go a long way in showcasing its capabilities.

Threats

With its big-data capabilities that the company says can cover entire countries, Anubis could find itself restricting its market to just the largest of telcos or governmental departments. Unless it can demonstrate a real value-add to enterprises' SIEM products, battling them could prove to be difficult.

Reproduced by permission of The 451 Group; © 2013. This report was originally published within 451 Research,Â’s Market Insight Service. For additional information on 451 Research or to apply for trial access, go to: www.451research.com