imVision Anomaly Detection Platform

New Operational & Security Challenges with Network Function Virtualization

Although Network Function Virtualization (NFV) brings many benefits to Telco service providers, including significant reductions in Capex and Opex, increased automation and shorter time to market of new services, it also makes the detection of network's anomalies much more challenging.

For service providers, network anomalies may appear due to two major reasons:

- **Operational** – misconfiguration of an entity in the network, software bugs or malfunctions, unexpected loads, etc.
- **Security** – external or internal attacks on network's infrastructure, causing disruption to network services, gathering confidential information, etc.

In a virtualized and decomposed NFV environment, the process of detection, diagnosis and corrective actions can prove to be long and costly. The stages include detection mechanisms, affected entity identification, problem isolation, anomaly analysis and resulting corrective actions. With an automatic detection and isolation technology, this process can be significantly shortened, while providing more precise and detailed analysis.

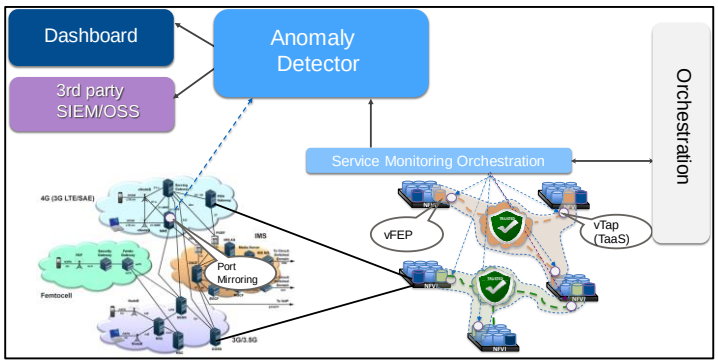
Service Aware Anomaly Detection

Applying a unique combination of expertise in networking as well as cyber security and machine learning, imVision's solution is the first and currently only available service-aware, network-based Anomaly Detection Platform (ADP), applicable to NFV, hybrid and legacy network environments.

Through an efficient and native architecture of virtual taps (vTAP) and virtual front-end processors (vFEP) that are tightly coupled with NFV's Network Management and Orchestration (MANO), ADP monitors the control and management traffic for all the entities/functions relevant a specific Network Service. By correlating behavior between entities, the platform is able to detect quickly and efficiently any anomaly in the service interactions, and provide in depth analysis to the cause of such anomaly.

The ADP core technology is based on the following elements:

- Advanced learning mechanisms to thoroughly study the specific behavior of each network entity.
- Correlative Behavioral Analysis (BA) algorithms, leveraging the deep expert knowledge of each network service
- Anomaly Detection in all types of Telecom services and in all network environments



ADP is provisioned with a "Golden Model" of each Network Service. This abstract model contains a predefined set of behavioral rules and an incidents' repository. The Golden Model is augmented with service and resource data that is specific to a particular deployment and is continuously being learnt from MANO. A learning phase facilitates the platform's adoption to specific vendor(s) and network scenarios, analyzing fine-granularities of the distinct procedures and messages and fine tuning the platform thresholds to the network's statistics.

By understanding the protocols and procedures of familiar network services, a Correlative BA platform like ADP provides significant added value compared to General BA systems or traditional OSS-based correlation solutions.

About imVision Technologies

imVision Technologies was established in 2014 by a team of veterans from the Telecom and cyber security markets. Backed by two leading VC's, the team includes professionals from multi disciplines including Telco Networking, cyber security, anomaly detection and Machine Learning.