Service-Aware Anomaly Detection Platform

Solution Description

Executive Summary

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

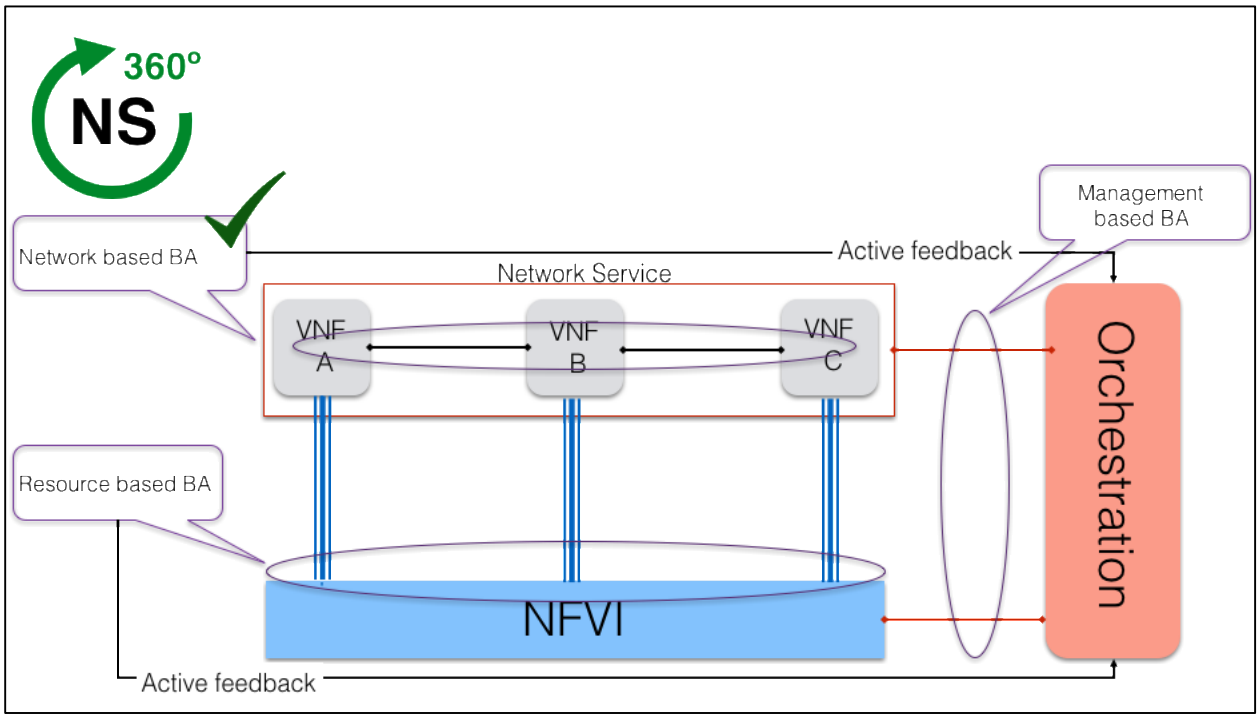
imVision's solution, the Anomaly Detection Platform (ADP), is a software product installed by the Telco Service Provider, providing a detection and analysis mechanism for anomalies in the network. The platform provides an automatic root-cause-analysis which can be displayed either on the platform's dashboard or on the operator's existing management systems through standard APIs.

imVision's solution is targeting Tier-1 Telco operators running either legacy physical networks, Telco over Cloud networks such as NFV/SDN, or are on a migration process with a hybrid approach of both legacy and cloud. The solution was initially developed for mobile networks, however it can be easily customized to other networks, such as fixed or enterprise, should there be a need.

The platform is currently being evaluated by several Tier-1 operators globally, with additional PoCs planned in the following months.

imVision's Anomaly Detection Platform (ADP)

The ability to provide an accurate root cause analysis and a complete description of the anomaly relies on the collection and correlation of all available information in the network. The Anomaly Detection Platform supplies the Service Provider with a 360° view of the Network Service. This holistic view is achieved by correlating the behavioral analysis of the network service itself with Resource based Behavioral Analysis derived from the infrastructure, and Management based Behavioral Analysis stemming from the Orchestration.



Through its unique combination of expertise in networking as well as cyber security, imVision's solution is the first and currently the only available Service-Aware Anomaly Detection Platform.

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

- Operational –misconfiguration of an entity in the network, software bugs or malfunctioning, or unexpected loads, may cause operational issues.
- Security – an external (to the network) or internal attacks on network infrastructure, causing disruption to network services, gathering confidential information, fraud purposes, etc.

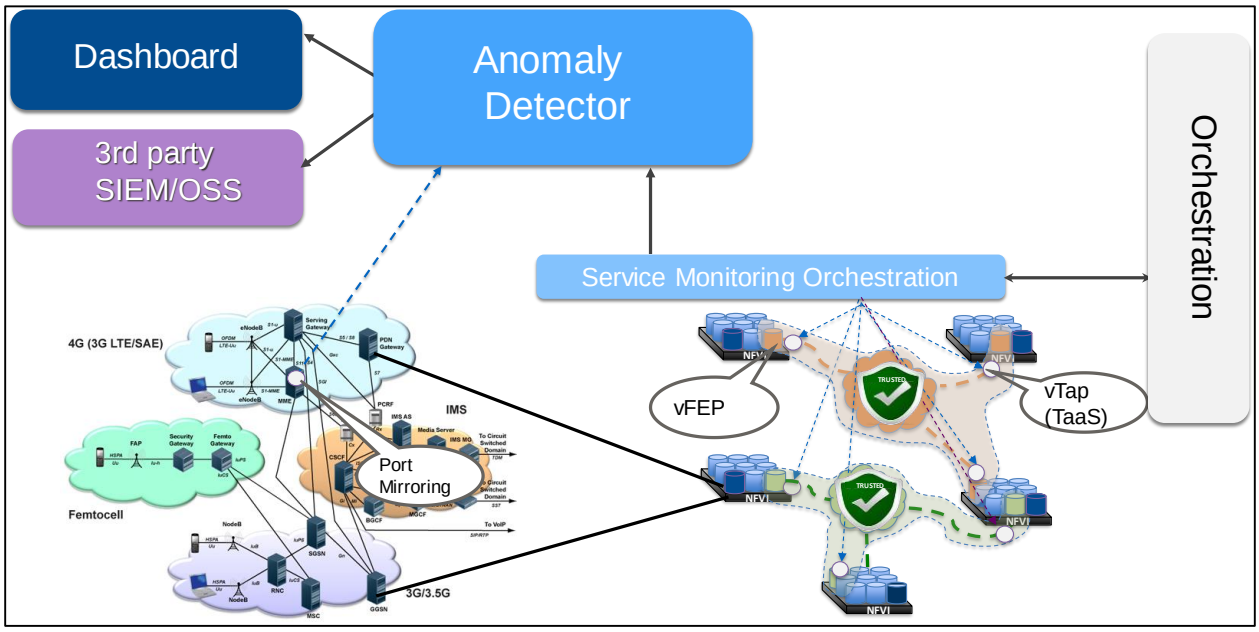
In many cases, the process from detection and up to the stage where corrective actions can be taken, can prove to be a long and costly process. The process stages include a detection mechanism, affected entity identification and problem isolation, anomaly analysis and resulting corrective actions. This complication can cause service interruptions and affect customers' experience. With an automatic detection and isolation technology such as imVision's ADP, this process can be significantly shortened while providing better analysis.

The ADP platform is developed as an open architecture, which simplifies its integration into an existing network infrastructure and connecting it with 3rd party management systems. Its core technology is based on the following elements:

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

Architecture

Detecting anomalies in the behavior of a Network Service requires continuous examination of traffic patterns related to that service. The Anomaly Detection Platform monitors the control and management traffic passing through all the entities relevant to the specific Network Service. By correlating traffic patterns between entities, the platform is able to detect quickly and efficiently any deviations in volume proportions between the entities and provide in depth analysis to the cause of the deviation.



The Anomaly Detection Platform in a virtualized network scenario, includes a Service Monitoring Orchestration (SMO) layer. The SMO instantiates a single vFEP (virtual Front End Processor – responsible for turning the network's raw data into meta data) per host machine, and connects it to local vTaps in order to avoid sending raw data outside the host machine. The vFEP extracts the metadata, encrypts it and sends it to the Anomaly Detector module for processing. In the case of a legacy/physical network, Port Mirroring is used instead of vFEPs and vTaps, in order to mirror traffic to the Anomaly Detector module directly.

Unique Value Proposition

Through its 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).

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

- Operational –misconfiguration of an entity in the network, software bugs or malfunctioning, or unexpected loads, may cause operational issues.
- Security – an external (to the network) or internal attacks on network infrastructure, causing disruption to network services, gathering confidential information, fraud purposes, etc.

In many cases, the process from detection and up to the stage where corrective actions are taken, can prove to be a long and costly process. The stages of such process include a detection mechanism, affected entity identification and problem isolation, anomaly analysis and resulting corrective actions. This complication can cause service interruptions and affect customers' experience. With an automatic detection and isolation technology such as imVision's ADP, this process can be significantly shortened while providing better analysis.

The ADP platform is developed as an open architecture, which simplifies its integration into an existing network infrastructure and connecting it with 3rd party management systems. Its core technology is based on the following elements:

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

Virtualization – The Challenge for Telco Service Providers

Although virtualization brings many benefits to the service providers, including significant reductions in Capex and Opex, increased automation and shorter time to market of new services, it also poses new challenges, especially from operations and security perspectives. These challenges must be addressed in order to assure a smooth migration path from the legacy physical networks to the virtualized domain, as well as maintain a healthy and efficient virtualized environment at the end of the migration process.

One of the main operational challenges is the fact that for a significant period during the migration phase, legacy and NFV architectures must co-exist with heterogeneous networks made up of both NFV and legacy elements working side-by-side.

In addition, similar to other cases of introducing new technologies and philosophies, a knowledge gap is automatically created in transformation and adoption to the new architecture. Not only a knowledge gap is created, but there is also a fundamental reshaping of the operator's skills set which needs to be bridged in order to ensure a smooth and efficient migration and roll out of services.

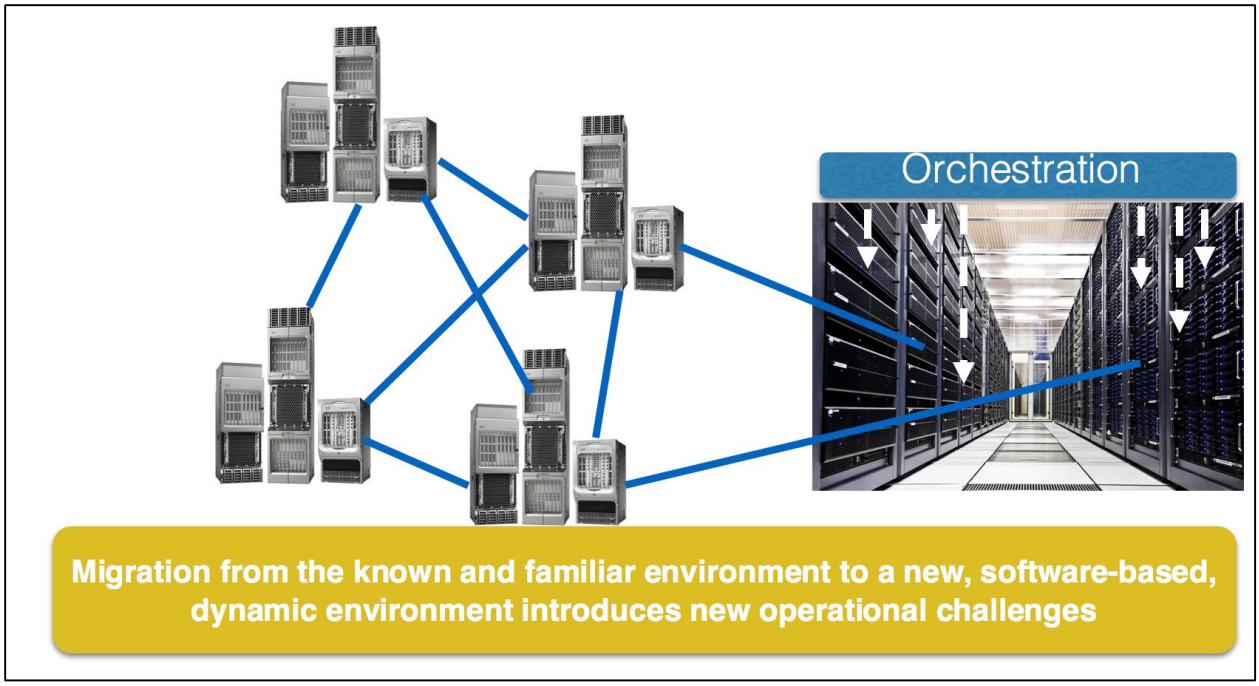
On the security side, the complete separation between control and data planes and the decoupling of services from the infrastructure, mean that a deeper level of defense mechanism is required to protect the network services and infrastructure.

Also, new security focal points such as the Orchestrations and Controllers that are required in a virtualized environment, create new vulnerable locations in the network, which, if compromised, can affect the entire Network's functioning. Finally, the use of COTS (Common Off the Shelf) Hardware and Open Source Software poses an increased risk of security holes that need to be addressed.

Impact on Operability

Migration from network element-centric to software-centric operations will drive fundamental changes in the network operating models across multiple dimensions: tighter integration across networks will be required, establishing new teams trained to handle and maintain the hybrid network's architecture, as well as incorporating new management tools.

For effective management of services in the virtualized environment, where performance is highly dependent on underlying cloud infrastructure, self-learning and predictive techniques must be developed to manage end-to-end service performance by intelligently correlating inputs at all levels and across different locations.



Early fault detection and mitigation is key to deliver carrier grade service availability and improve end user's experience. With the ability to proactively correlate physical and virtual faults at a service level and performing VNF/network topology reconfiguration, Mean Time to Repair (MTTR) can be greatly reduced.

Impact on Security

Transition to NFV carries significant changes from the traditional hardware based core networks of the operators. The main differences are:

- A shift towards a generic hardware while implementing most of the functionality of the network in software while using a lot of open source code. These changes are likely to make the network more vulnerable to Cyber-attacks, compared to existing networks comprised of proprietary based hardware and software network elements.
- Decomposition of core network functions along with dynamic network configuration: This change will make the network much more complicated visibility-wise, will bring in new protocols and will expose a lot of what used to be an inside-the-box communication between modules, to an IP network communication between VMs.
- New security focal points such as the MANO and the SDN controller: these focal points may be hot targets for an attack, if compromised can affect the entire NS.

The above mentioned changes will make the Service Provider’s network more complicated to manage. Traditional security measures such as Firewalls and IPSs are still required, but they do not address the specific changes caused by the transition to NFV. In order to assure operator's ability to secure the Network Service and be able to have visibility and understanding of security in the Network Service a new solution is required.

Physical Telco Network

Hard to attack
- Unique knowledge
- Unique attack tools

Proprietary HW

Proprietary OS

Proprietary SW

Virtualized Telco Network

Easy to attack
- Common knowledge
- Common attack tools

Off the shelf HW

Common & open OS

Open source SW

Attacking Network Function in Telco cloud is as easy as attacking any application server in the IT cloud