keynetic

flowCortex

ML-based security solution

The highlights

- flowCortex enables the automated discovery of assets and security policies through advanced **Artificial Intelligence and Machine Learning (AI/ML)** techniques.
- It allows you to start securing your network quickly through non-intrusive techniques, letting you **easily understand the underlying dynamics**.

Discover your assets easily

The first step in securing a network is identifying what devices are connected to your infrastructure and the kind of traffic they exchange. This task usually requires technical experts with industrial, network and security background, and the utilization of intrusive mechanisms, such as port monitoring.

Discover your assets automatically and let the system group them and refine their security policies for you with our light and easy-to-deploy component.

Security and network intelligence

With flowCortex, you can benefit from the most advanced AI/ML techniques to quickly and easily identify your network assets and traffic patterns. flowCortex gathers traffic information using widely adopted standard protocols available in the networking devices. Once the data is gathered and processed, flowCortex lets you know what kind of traffic flows are being exchanged through the network.

Our Machine Learning technology allows you to gain a quick understanding of the network dynamics and the interactions between your devices **without investing any effort**. Having full knowledge of your network and the exchanged traffic allows you to make **smarter and more efficient decisions.**

Smart traffic profiling

With flowCortex you can **automatically characterize** all the devices connected to your network, so as the traffic flows associated to the different groups within your organization. This capability of flowCortex facilitates the accurate definition of security policies and the adoption of best practices.

By automating this process, our clients can **reduce the time and effort** required for the correct characterization of the environment being controlled. There is no need to define network access policies manually again, neither to characterize devices or groups. In addition, you can integrate flowCortex and flowNAC, improving the security of your network and simplifying the security policy creation.

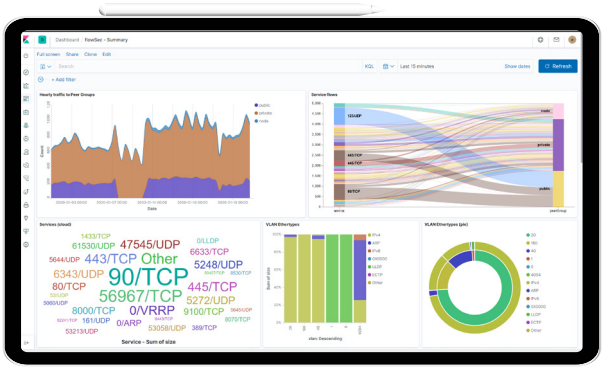
Anomaly detection

flowCortex is continuously learning from your network, allowing you to have a clear and updated view of ongoing interactions between the assets. It also enables **anomaly detection**, since the traffic exchanged through the network is known and can be compared with previous traffic pattern snapshots.

With flowCortex, you will be **immediately notified** of any change out of the ordinary inside your

network, giving you a precious extra time to implement the necessary countermeasures.

Moreover, by jointly using flowCortex with flowNAC, our identity-based Network Access Control solution, you can even automate the necessary countermeasures.



The **benefits**

- Reduce time and effort needed during the deployment phase through the automatic discovery of assets and traffic flows between them, thus saving costs.
- Clear understanding of traffic flows exchanged through the network.
- Automatically classifies the devices connected to the network and the exchanged traffic flows, aggregating the assets and their interactions according to business processes.
- Updated inventory of all the connected assets to reduce risk, actually achieving an auditable system.
- The system is continuously learning.
- Accelerates the securing of your network through ML technology to quickly and easily define security policies.
- Continuous analysis of your network for anomaly detection to speed up the execution of the necessary countermeasures.

About us

Keynetic is an innovative cybersecurity SME that develops their own products for network security and intelligence by leveraging the most advanced Software-Defined Networking and Network Functions Virtualization (SDN/NFV), Network Automation and Machine Learning technologies.

We envision network security as an iterative process – visualization & control – that begins with the understanding of the network dynamics and the interactions between your devices. The actual data extracted from the network devices guides this procedure. Thanks to ML technology the time and effort invested in this process is drastically reduced.