keynetic

flowNAC
SDN-based security solution

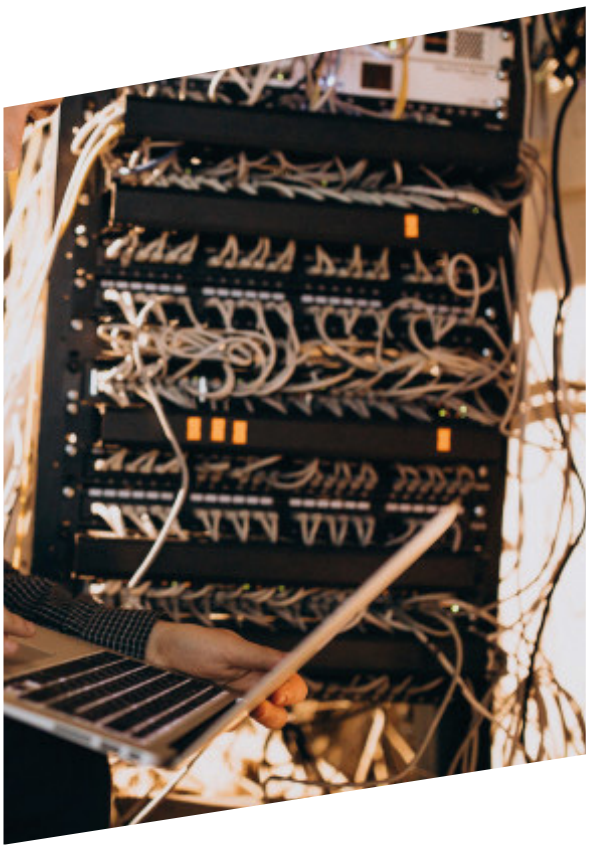
The **highlights**

- flowNAC is a highly flexible and extensible **network security solution** that allows to control the access to authorized services based on the identity of the users.
- It improves the security of industrial networks simplifying the associated management relying on two principles: **visualization and control**.
- Our solution **reduces the risk** of exposing critical production assets to cyberattacks in a smple an automated manner.
- It allows to define which specific services are granted for each authenticated device through **micro-segmentation**.

New industries with new security challenges

The industrial sector is facing an exciting transformation towards Industry 4.0. The digitalization of the factories is the enabler of this innovation, in which communication networks become fundamental. There are plenty of benefits and opportunities, such as predictive maintenance, Big Data applied to more efficient industrial processes, or teleassistance. However, the interconnection of machines and devices creates new risks and threats, as traditionally isolated devices now connected to IT resources become exposed to cyberattacks. In industrial environments, the lack of availability due to a security threat is unacceptable since the production cannot stop.

Current recommendations for industrial network security (such as IEC 62433, ISA99 and NIST800-82r) are based on **defense-in-depth and segmentation strategies**. Network segmentation relies on the definition of trusted segments, meaning that a device is trusted just because it is connected to the segment. As a result, if a single device is compromised inside the segment the full segment is compromised.



Visualize and control your industrial network with flowNAC

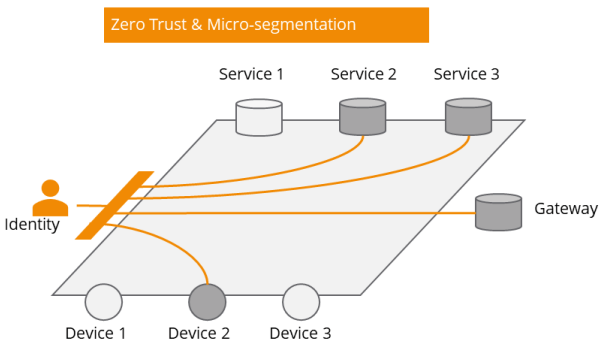
flowNAC has been designed to **improve the security** of industrial networks through an **iterative process** built on top of **visualization and control** capabilities. flowNAC exposes an updated dashboard showing who is connected to the network and controls the services granted for each device, and all this without impacting the production.

flowNAC **simplifies security management** by centralizing all associated processes to automatically deploy the resulting security policy leveraging the most advanced SDN and Network Automation technologies.

Instead of using complex network parameters, security policies are defined in business logic to simplify both the management and the communication between the IT and business departments. Thanks to SDN technology, flowNAC allows to easily translate high-level intents (what I want) to low-level and fine-grained policies (how to make it) and automatically deploy the security policy.

Zero-trust model and micro-segmentation for increased security

flowNAC takes advantage of one of the latest trends in networking technologies, called , to provide a cutting-edge solution to this problem. It entails a paradigm shift, since it evolves the trusted segment model into a Zero-Trust model, increasing the security of the connected assets. In addition, flowNAC allows to define which services are granted for each authenticated device, known as micro-segmentation.



flowNAC takes advantage of one of the latest trends in networking technologies, **Software Defined Networking (SDN)** and Network Automation, to provide a cutting-edge solution to this problem. It entails a paradigm shift, since it evolves the trusted segment model into a **Zero-Trust model**, increasing the security of the connected assets. In addition, flowNAC allows to define which specific services are granted for each authenticated device through **micro-segmentation**.

With flowNAC, neither a malicious device, nor the unauthorized traffic coming from a compromised device are able to access to the network, thus, **preventing lateral movement** and protecting all the machines connected to the factory with additional barriers.

Start using flowNAC and take advantage of our **progressive deployment plan** adapted to you.

The **benefits**

- Reduce the risk of exposing critical production assets to cyberattacks in a simple and automated manner.
- Reduce the attack surface exposed by your factory with a Zero-trust model and network micro-segmentation. flowNAC enables the hardening of the industrial network by limiting the lateral movement inside the segment following a whitelist approach to restrict the propagation of threats and malware.
- Reduce time and effort through security automation and centralized orchestration of all the security elements spread across the factory to enforce the security policy.
- Simplify the security management with a centralized definition of security policies in business logic, assuring a coherent definition adapted to the industrial processes.
- The system becomes auditable with updated information on the actual security definition, while tracking each and every change. flowNAC also provides an updated and clear view of all the connected devices.
- Smooth improvement of overall security through an interactive process – vision & control – that allows you to take the control of the network security in a comprehensive manner.
- Supports event-driven access updates based on external parameters, such as time, geolocation, or alarms.
- Highly flexible and extensible network security solution that ensures a homogeneous security level for every device connected to the network, since it does not depend on end-systems' security. This is especially relevant for the industrial sector with very heterogeneous machines and devices, with different capabilities and non-updated systems.
- Allows our customers to know their networks and improve the protection of their connected assets in an understandable way with a solution tailored for the industrial sector.

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.