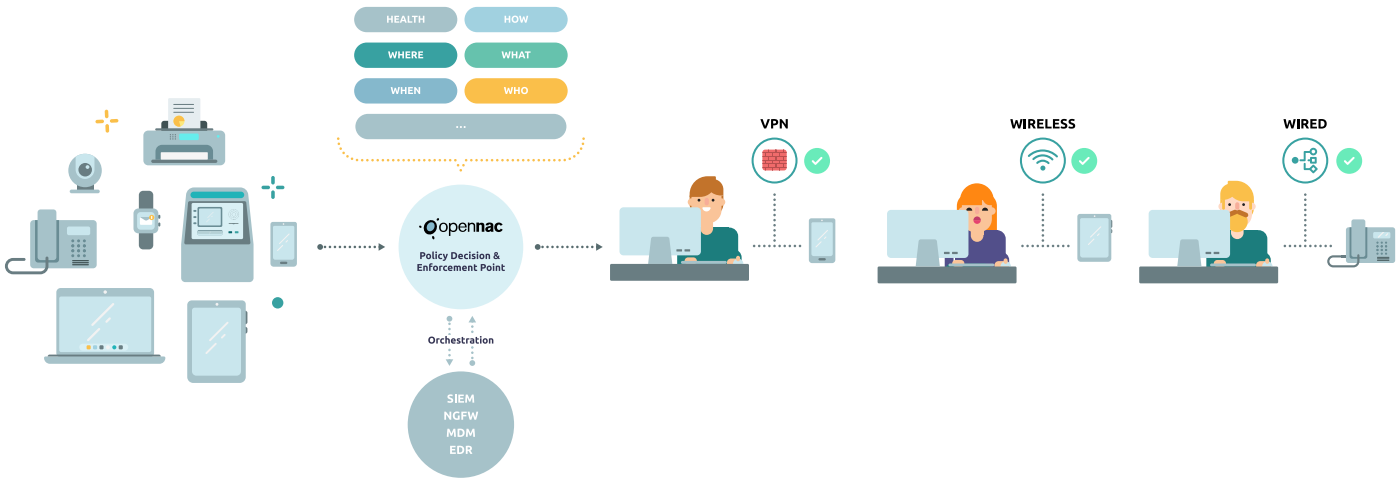
Visibility and control of all assets: the security base



Threat detection time has fallen on average, however, the response time and the impact of disruptive attacks (Business Disruption Attacks) continues to grow due to lack of asset visibility and control. In addition, pressure from auditors and regulations regarding the assets connected to the corporate network continues to grow.

Laptops, smartphones, tablets, suppliers, external users, and an avalanche of IoT devices are connected daily to networks that are increasingly heterogeneous, dispersed and complex to manage, each asset is a potential attack or recognisance point.

Our solution openNAC Enterprise, regardless of the type of device and how it connects to the network, automatically discovers and profiles all assets connected to your network.

Do you have visibility and control of all assets connected to your network? And can you prove it in an audit? The asset (entity and / or identity) should be the first line of defense.

At Open Cloud Factory we increase network security by enabling organizations 100% visibility and control of all assets connected to the (Wireless, Wired and / VPN) network at all times.

Solution: openNAC Enterprise

Through centralized visibility and control that brings our openNAC Enterprise solution can reduce the risk and impact of disruptive attacks and respond to regulatory requirements. **openNAC Enterprise**, regardless of the type of device and how it is connected, automatically discover and categorize all assets. Organizations can apply the categorization the context of the business and its risks to prioritize their efforts and respond to audits etc.

Having gained visibility solution provides a single point where you can define and apply access policies tailored to the needs of the organization, and rights for all connected assets and attempting to connect. The same is achieved multiple mechanisms.

openNAC Enterprise is a software solution can be deployed from the cloud, on-premise or a hybrid model thus reducing the impact on your infrastructure.

- We can use 802.1x many other mechanisms to authenticate, authorize and audit; with / without agent, span port, SNMP Traps, Open Ports.
- We adapt to electronic multivendor environments.
- Having a central point for the definition and implementation of policies for access to the network for users, devices and dramatically reduces management costs, but also creates applications uniformed security posture.
- With the orchestration security you get more out of your current security investment. Use integrations / third party information (Siems, NGFW, AVs, EDRs, MDGs ..) for policies with more context and information sharing solution for others.

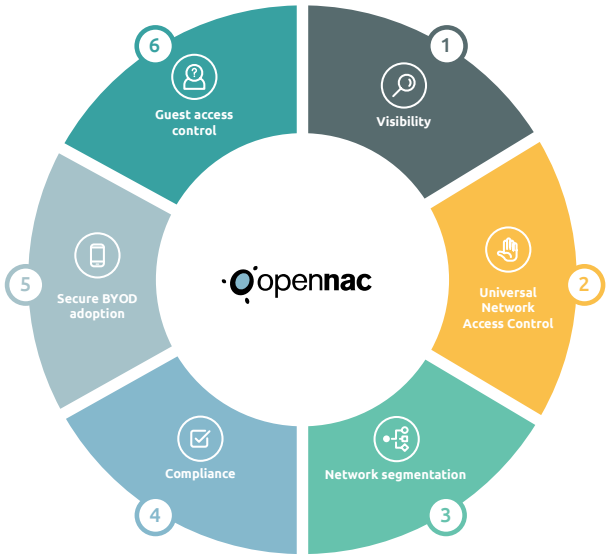
Visibility and control assets is the security of CIS No. 1 *

*Center for Internet Security https://www.cisecurity.org

The modular solution that meets your needs today and tomorrow:

openNAC Enterprise is a solution that provides visibility and control over corporate networks. With **openNAC Enterprise** you will discover all devices (being the size they are) that are connected to their infrastructure, offering different mechanisms for discovery, profiling and control access to your network.

In addition, **OpenNAC Enterprise** is the only solution that provides the security modules. Providing the best security that fits your current situation, providing results in less time and with less effort. The modularity of our solution could increase as the maturity of the security posture of your organization.



VISIBILITY

- Device Inventory 100% / things, infrastructure and users.
- Automatic continuous visibility into the connection.
- Tagged critical assets (GDPR etc.) by business context and risks related to prioritize cybersecurity efforts.
- It allows audits and respond to attacks.

UNIVERSAL ACCESS CONTROL

- Simplify access control assets wired networks, Wi-Fi and Virtual Private Networks (VPN)
- Single point of decision and implementation of access policies.
- Integration / adaptation with other security solutions NGFW / SIEM etc.

NETWORK SEGMENTATION

- Segmenting networks and functions to contain the damage when an intrusion occurs.
- Reduce the attack surface.
- Protect / isolate critical assets.
- Simple segmentation of IoT.

COMPLIANCE

- Ensure infrastructure complies with corporate / regulatory policies.
- Define and enforce security baselines for Eps, Datacentres and Network Devices (switches and access points).
- Respond rapidly to vulnerabilities and enforce mitigation / contention.
- Permanent (staff) and dissolvable (third parties) agents for granular EP control“

SAFE BYOD

- Unique corporate identity
- Monitor and track network access

CONTROL OF ACCESS TO INVITED

- Automatic network isolation
- Reconfiguring access.

Nonintrusive / all inclusive

- **Different deployments:**

  From the cloud: The cloud deployment requires no infrastructure or mantenimiento.

  Onpremise: VMs requires no on-premise hardware.

- **Horizontal scaling**
- **Multivendor environment friendly / Agnostic**
- **It fits your network infrastructure without HW / SW updates and update**