Visibility: The prerequisite to security

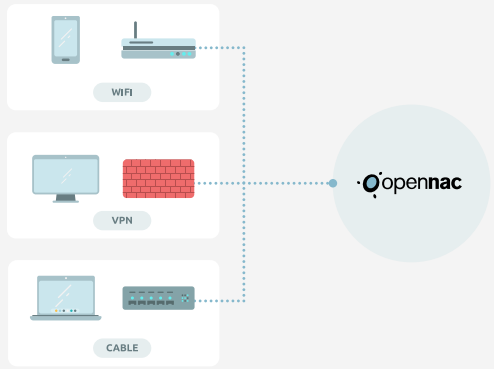
By 2020 there will be **more than 30 billion* connected devices**, the immense majority will be light and will not have the capacity to install standard security controls. As these devices are purpose-built and "user friendly", generally plug and play, lots of business units will purchase and implement them without provisioning them with network and security operations first.

Each one of these blind spots is a potential attack and or reconnaissance point.

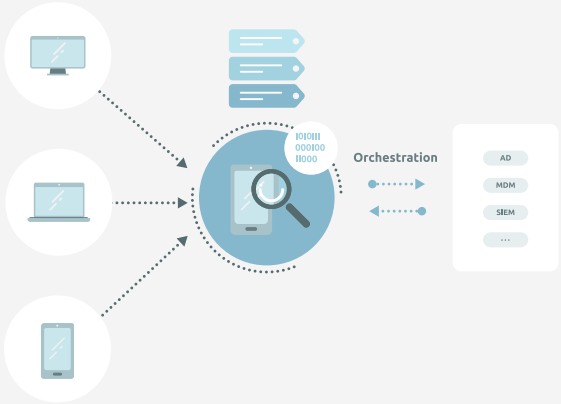
If we add the IoT Tsunami to the status-quo of dispersed offices, remote staff, service providers / collaborators, BYOD, implementing the new while maintaining the old on heterogenous electronics it is no wonder regulators and auditors are pressuring organization to have greater visibility of devices that are connecting to the network.

Asset visibility and control is CIS's Nº1 security control**

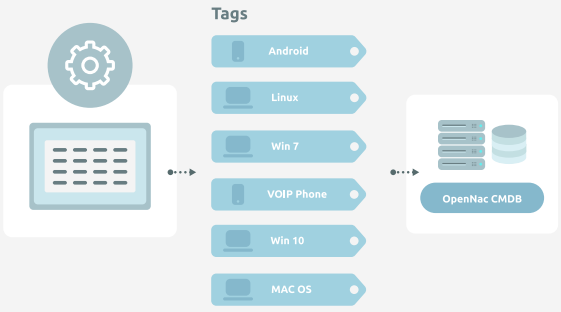
1. Discovery



2. Profiling



3. Register



4. Value

* https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

** CIS (Center for Internet Security, Inc.) is a non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats https://www.cisecurity.org

Why openNAC Enterprise visibility?

As **openNAC Enterprise** is a **software-first solution** it enables organizations to get **every device** discovered and profiled with minimum impact to the network and then add layers of additional visibility and control to fine tune the security stack as required.

Visibility is gained on all assets across all access layers; cable, wi-fi and VPN. Visibility is real-time, on connection, and is continuous. In addition to state changes, which will force an assets review, you can also establish periodic review periods.

As the solution is **software-first** it is natively adaptable.

- It is vendor-agnostic
- Applicable to 802.1x and non-802.1x assets
- Agent and agentless
- Uses active and passive techniques to gain maximum insights / context
- Adapts to multiple identify sources
- It's asset information can be easily extended to apply business logic manually or via integrated third parties
    - » Establish critical nature of the assets to facilitate policy enforcement and reports to respond to audit requirements or breach management

All of this information is processed via restful APIs. This means that information is easily consumed by third parties, such as SIEMs, to give them greater context and help organizations leverage their existing security stack.

The information is fed to the centralized policy decision and enforcement point to apply granular controls. These controls respond directly to the organizations needs as the business logic is integrated into the assets information.

Visibility modes

Organizations can implement one or all three of the following visibilities modes.

Name		Network Device Mode	Sensor Mode	Agent Mode
Source		Layer 1-4	Layers 2-7	Operating System
Network Traffic Visibility			Deep packet network traffic inspection	
Asset Visibility	Discovery	802.1x accounting events DHCP requests events MAC Table for switches and routers SNMP Traps events Custom reader	Sensor connects to the network device via port span this device collects multiple application-layer protocols including DNS, DHCP, FTP, HTTP, IRC, SMTP, SSH, SSL... to discover devices.	Installing an agent on endpoints offers in-depth information on endpoints including full hardware and software inventory. This information can enrich both the Network Device and Sensor Mode and the agent can also enables fine tune enforcement policies.
	Profiling	MAC Vendor HTTP Banners / Requests etc. Service information SNMP queries Banner Port information DHCP fingerprinting Operating System fingerprinting + Granular SW / HW inventory + Services, processes + Security posture (patching, app status…)		

Profiling using Tags and Types

Types

By default, **openNAC technologies** include the capabilities to detect the type of devices connected to the network based on different tools and processes, this is called asset profiling. There are two methods for profiling:

1. **Automatic profiling:** The system includes out of the box profiling rules that are updated frequently to cover the great majority of device types; IP Cameras, Desktops, Mobiles, IP Phone etc.

2. **Manual profiling:** The administrator can define profiling rules manually with a few clicks to expanded the set to respond to and define specific device types (assets) connected to the network using some of the following methods; DHCP Fingerprint, Ports, Banner, SNMP Service Information HTTP, MAC vendor, OS.

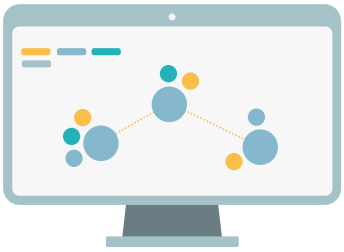
Tags

As the number and type of devices grow exponentially it is critical that a flexible system is in place to horizontally adapt to that growth. **openNAC** uses Tags to profile devices. Tags represent device characteristics, such as IP, MAC, Vendor, Port ID etc. these are examples of structured data per device but also creates, on the fly, unstructured Tags to adapt to the growing amount of device information (device type, open ports, security information…)

All asset information is stored in a CMDB, which stores all characteristics and attributes in a flexible schema that can be easily expanded manually and or via third party information. Organization can apply business logic via Tags to identify critical assets, IoT categories etc.

Profiling is done using multiple mechanisms depending on the type of deployment that an organization requires. The Tags are then leveraged to create access policies and establish controls.

How can you leverage the data



Business profile Dashboards

Group different policies then identify the assets that match with these network access rules. Very helpful for upper management high-level progress status of a given situation

CMDB view

Leverage the internal CMDB by applying filters; structured (Vendor, MAC, Host Name, Owner…) and unstructured tags (Device type, open ports, security status…)

Free search on Analytics Engine

openNAC Analytics module provides a powerful search engine, allowing you to openly search any data, this is crossed with all information (asset, traffic etc.)

Non-intrusive / all inclusive

- **Cloud deployment requires zero infrastructure or maintenance.**

  VMs on-premise requires no HW.

- **Scales horizontally to meet changing needs.**
- **Multivendor friendly / vendor agnostic.**
- **Adapts to your network infrastructure, no need for HW / SW updates and upgrade.**
- **Control access via all access layers (Wi-Fi, Cable, VPN and Apps)**