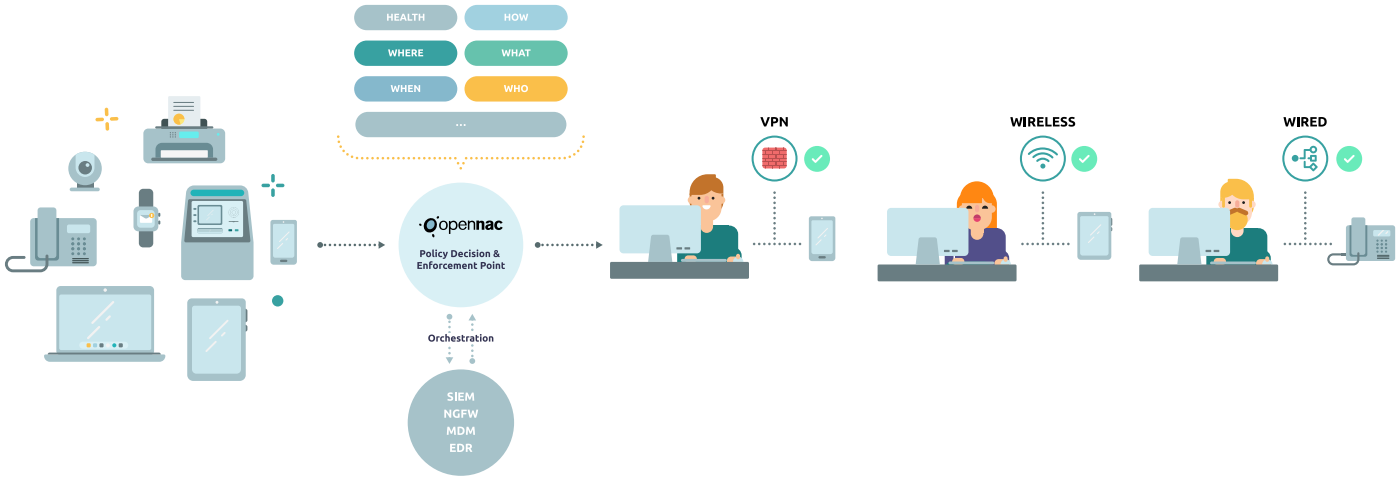
Visibilidad y control de los activos: la base de la seguridad



El tiempo de detección frente a un ataque ha bajado de media, sin embargo el tiempo de respuesta y el impacto de ataques disruptivos (Business Disruption Attacks) sigue en crecimiento debido a la falta de visibilidad y control de los activos. También al alza van las exigencias de los auditores y regulaciones en cuanto a los activos conectados a la red corporativa.

Portátiles, smartphones, tablets, proveedores, usuarios externos, y una gran oleada de dispositivos (IoT) se conectan diariamente a unas redes que son cada vez más heterogéneas, dispersas y complejas de gestionar, cada activo es un riesgo a gestionar.

Nuestra solución openNAC Enterprise, sin importar el tipo de dispositivo y cómo se conecta, automáticamente descubrirá y categorizará todos los activos de su red corporativa.

¿Tienes visibilidad y control de todos los activos conectados a tu red? ¿Y puedes demostrarlo en una auditoria? El activo (entidad y/o identidad) debería ser la primera línea de defensa.
En Open Cloud Factory incrementamos la seguridad de la red permitiendo que las organizaciones tengan una visibilidad y control 100% de todos los activos que se conecten a la red (Wifi, Cableada y / VPN) y en cada momento.

La Solución: openNAC Enterprise

A través de la visibilidad y control centralizado que aporta nuestra solución **openNAC Enterprise** podrá disminuir el riesgo y el impacto de los ataques disruptivos y responder ante requisitos de regulaciones. **openNAC Enterprise**, sin importar el tipo de dispositivo y cómo se conecta, automáticamente descubrirá y categorizará todos los activos. Las organizaciones puedan aplicar la categorización al contexto del negocio y sus riesgos para priorizar sus esfuerzos y responder ante auditorias etc.

Una vez conseguida la visibilidad la solución le proporciona un punto único donde puede definir y aplicar políticas de acceso, adaptadas a las necesidades de la organización, y los derechos correspondientes para todos los activos conectados y que intenten conectar. Lo mismo se consigue de múltiples mecanismos.

openNAC Enterprise es una solución software se puede implementar desde la nube, on-premise o en un modelo híbrido reduciendo así el impacto en tu infraestructura.

- Podemos usar 802.1x y muchos otros mecanismos para autenticar, autorizar y auditar; con / sin agente, port span, SNMP Traps, Open ports.
- Nos adaptamos a los entornos de electrónica multivendor.
- Tener un punto de central para la definición y ejecución de políticas para el acceso a la red para usuarios, dispositivos y aplicaciones reduce drásticamente los costos de administración, pero también crea una postura de seguridad uniformada.
- Con la orquestación de seguridad sacarás más provecho de tu inversión en seguridad actual. Usar integraciones / información de terceros (SIEMs, NGFW, AVs, EDRs, MDMs..) para que las políticas tengan más contexto y compartir información de la solución para que otras

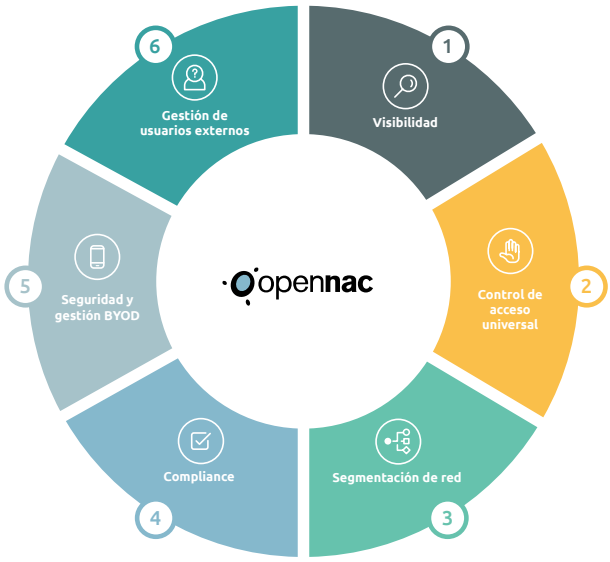
La visibilidad y el control de los activos es el control de seguridad Nº1 de la CIS*

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

La solución modular que responde a tus necesidades hoy y mañana

openNAC Enterprise es una solución que ofrece visibilidad y control total sobre las redes corporativas. Con **openNAC Enterprise** descubrirá todos los dispositivos (siendo del tamaño que sean) que están conectados a sus infraestructuras, ofreciendo diferentes mecanismos de descubrimiento, perfilado y control acceso a su red.

Además, **OpenNAC Enterprise** es la única solución que ofrece la seguridad por módulos. Proporcionando la mejor seguridad que se adapta a tu situación actual, aportando resultados en menos tiempo y con menos esfuerzo. La modularidad de nuestra solución podría incrementarse a medida de la madurez de la postura de seguridad de tu organización.



VISIBILIDAD

- Inventario 100% de dispositivos / things, infraestructura y usuarios.
- Visibilidad continua automática en la conexión.
- Etiquetar activos críticos (GDPR etc.) por contexto del negocio y los riesgos de ciberseguridad relacionados para priorizar los esfuerzos.
- Permite responder ante auditorías y ataques.

CONTROL DE ACCESO UNIVERSAL

- Simplifique el control de acceso de los activos en redes cableadas, Wi-fi y redes privadas virtuales (VPN)
- Punto único de decisión y aplicación de las políticas de acceso.
- Integración /adaptación con otras soluciones de seguridad NGFW / SIEM etc.

SEGMENTACIÓN DE RED

- Segmentar redes y funciones para contener el daño cuando ocurre una intrusión.
- Reducir la superficie de ataque.
- Proteger / asilar activos críticos.
- Segmentación simple de IoT.

COMPLIANCE

- Asegurar que la infraestructura cumpla con las políticas corporativas / regulatorias.
- Definir y aplicar líneas de base de seguridad para Eps, Datacenters y dispositivos de red (conmutadores y puntos de acceso).
- Responder rápidamente a las vulnerabilidades y hacer cumplir la mitigación / contención.
- Agentes permanentes (personal) y solubles (terceros) para control granular EP”

BYOD SEGURA

- Unica identidad corporativa
- Controlar y rastrear accesos a la red

CONTROL DE ACCESOS INVITADOS

- Aislamiento automático de la red
- Reconfiguración de accesos.

No intrusivo / todo incluido

- **Diferentes depliegues:**

  Desde la nube: La implementación en la nube no requiere infraestructura o mantenimiento.

  Onpremise: VMs on-premise no requiere HW.

- **Escalado horizontal**
- **Entorno multivendor amigable / Agnostico**
- **Se adapta a su infraestructura de red, sin necesidad de actualizaciones HW / SW y actualización**