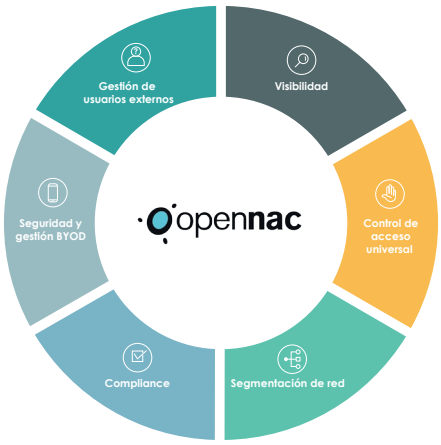
Visibilidad y control sobre la red

¿Qué es Emma?

Emma es una solución de seguridad para redes corporativas (tanto IT como OT) que permite a las organizaciones tener de manera centralizada la visibilidad, contexto, control y verificación del nivel de seguridad de todos los activos que se conectan a la red (Wifi, Cableada y VPN), desde dispositivos de usuarios a electrónica de red.

En la verificación del nivel de seguridad de los dispositivos de red, EMMA tiene integrado la lógica de ROCÍO. De este modo, se podrán hacer comprobaciones de manera centralizada.



¿Por qué Emma?

A través de la visibilidad, contexto y control centralizado que aporta EMMA, se puede disminuir el riesgo y el impacto de los ataques disruptivos y responder ante requisitos de regulaciones.

Al tratarse de una gestión centralizada, se reducen los esfuerzos de gestión y tiempos de respuesta.

Propiedades

Modular: su capacidad puede incrementarse conforme madura la postura de seguridad de la organización.

Flexibile: puede usar distintos mecanismos de visibilidad y control de dispositivos: 802.1x, SNMP Traps, Port Span, SFlow, Netflow, DHCP, Tablas MAC, con o sin agente etc, integrarse con AD, LDAP, 2FA (OTP, Mobile Connect) u otras soluciones (NGFW, MDMs, SIEMs).

Adaptable a la electrónica de red de distintos fabricantes.

Analítica: agregación de datos sobre activos, dispositivos, usuarios, eventos, accesos etc. Por tanto, permite obtener informes de trazabilidad así como integrarse con otras soluciones como ROCÍO.

¿Cómo funciona?

La instalación de EMMA requiere dos máquinas virtuales (Core y Analytics) y opcionalmente una tercera (Sensor). El Sensor es complementario y aporta una mayor visión del comportamiento de la red.

Core

- Motor de políticas
- CMDB
- Portal de administración

Analytics

- Motor de búsqueda
- Dashboards
- Informes

Sensor

- Decodificación de protocolos
- Comportamiento de red
- Port span / on-prem

Módulo de Visibilidad: para conocer todos los activos de nuestra Organización.

- Inventario continuo de dispositivos, infraestructura y usuarios en un CMDB centralizado.
- Etiquetado de activos críticos por contexto de la organización y riesgos de seguridad.

Módulo de Control y Segmentación: la identidad y autorización es la primera línea de defensa.

Simplificar el control de acceso de los activos en redes cableadas, Wifi y VPN.

- Punto único de definición y aplicación de políticas de acceso.
- Establecer controles de acceso a los dispositivos en función de su contexto y lógica de la organización.
- Integración /adaptación con otras soluciones de seguridad NGFW, SIEM, AD, LDAPs, 2FA, etc.
- Aplicar segmentación dinámicamente para reducir la superficie de ataque, aislar dispositivos críticos y responder ante ataques de manera centralizada.

Módulo de Verificación del nivel de seguridad (Compliance): para garantizar el cumplimiento de las políticas de seguridad de la Organización y del CCN.

- Comprobar la infraestructura mediante las reglas de verificación definidas en ROCIO.
- Definir y aplicar líneas base de seguridad para Endpoints y servidores (Datacenters).
- Agentes permanentes (personal) y solubles (terceros) para control granular de los Endpoints y servidores.

BYOD y acceso a invitados: mitigar riesgo de acceso de dispositivos BYOD o de terceros (Invitados).

- Uso de una identidad corporativa única.
- Controlar acceso en función del riego adicional y seguimiento de accesos.
- Gestión de invitados mediante un portal cautivo gestionable.
- Gestión de flujos de trabajo para sponzorizar invitados, por correo electrónico.