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 auge 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. Las compañías, para ser competitivas, se enfrentan a la paradoja situación de tener que transformar digitalmente, pero la misma transformación, mal gestionada, les abren unos riesgos sin precedentes.

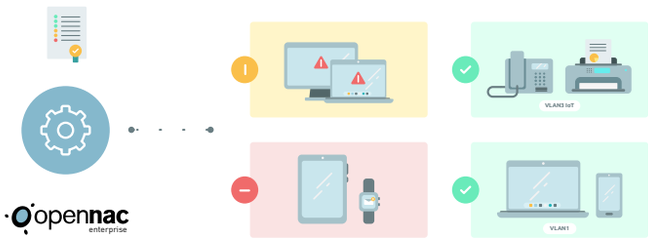
Portátiles, smartphones, tablets, proveedores y usuarios externos, y una gran oleada de dispositivos (IoT) se conectan diariamente a unas redes que son cada vez más heterogéneas, dispersas y complejas de gestionar, cada activo un riesgo a gestionar.

¿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.

NUESTRA SOLUCIÓN OPENNAC ENTERPRISE, SIN IMPORTAR EL TIPO DE DISPOSITIVO Y CÓMO SE CONECTA, AUTOMÁTICAMENTE DESCUBRIRÁ Y CATEGORIZARÁ TODOS LOS ACTIVOS.

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. Nuestra solución **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 de ciberseguridad 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.

Ya que **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.
- Podemos hacer todo esto independientemente de la capa de acceso: cable, Wifi, VPN, aplicación.
- Nos adaptamos a los entornos de electrónica multivendor.
- Puede implementar sin infraestructura adicional usando nuestra nube o puede usar una versión on-premise o un enfoque híbrido.
- 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.

VISIBILIDAD Y CONTROL: LOS DOS PRINCIPALES FACTORES QUE LE PERMITEN MANTENER SU RED CORPORATIVA 100% CONTROLADA

opencloud factory

LA SOLUCIÓN MODULAR QUE RESPONDE A TUS NECESIDADES HOY Y MAÑANA

OpenNAC Enterprise te ofrece la solución por módulos que se adapta mejor a tu situación actual permitiendo que veas resultados en menos tiempo y con menos esfuerzo. En la medida que vas madurando puedes agregar más módulos para responder a las nueveas prioridades.

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.

ENDPOINT COMPLIANCE

- Garantizar el cumplimiento de seguridad del EP con las políticas corporativas / mandatos regulatorios.
- Definir y aplicar políticas de seguridad para EPs.
- Descubrir EPs y garantizar el cumplimiento con la política de manera automática.

BYOD SEGURA

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

CONTROL DE ACCESOS INVITADOS

- Aislamiento automático de la red
- Reconfiguración de accesos.

Donde estamos ubicados

SPAIN

IMDEA Software Institute,Campus Montegancedo, S/N, Pozuelo de Alarcón, 28223 Madrid

BRAZIL

Market Place Tower I Av. Dr. Chucri Zaidan, 920 - 9º andar Cordeiro - São Paulo - CEP: 04583-904

MÉXICO

Presidente Masaryk 111 Piso 1, Miguel Hidalgo, Polanco V Sección, 11560 Ciudad de México

USA

Independence Wharf 470 Atlantic Avenue Boston, Massachusetts, 02210