Visibilidad, control y modularidad: seguridad de nueva generación

opencloud factory

Visibilidad, control y modularidad: seguridad de nueva generación

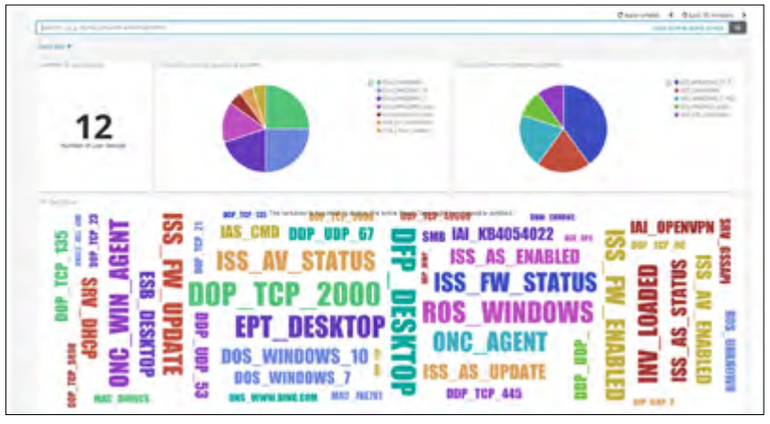
La red es un ente cada día más complejo, tanto dentro del perímetro, con un número incremental de dispositivos, conocidos o no, conectados a la misma, como fuera de él, donde se multiplican las conexiones con un sinfín de dispositivos móviles de empleados, proveedores y clientes, además de una cantidad ingente de dispositivos que todavía no ha llegado a su límite, o que, mejor dicho, todavía está por explotar, como es IoT.

Esto supone uno de los retos a los que las empresas deben enfrentarse cuando de seguridad hablamos, que se une a la necesidad imperiosa de cumplir con todas las normativas que afectan a las compañías, sus datos y sus sistemas de TI.

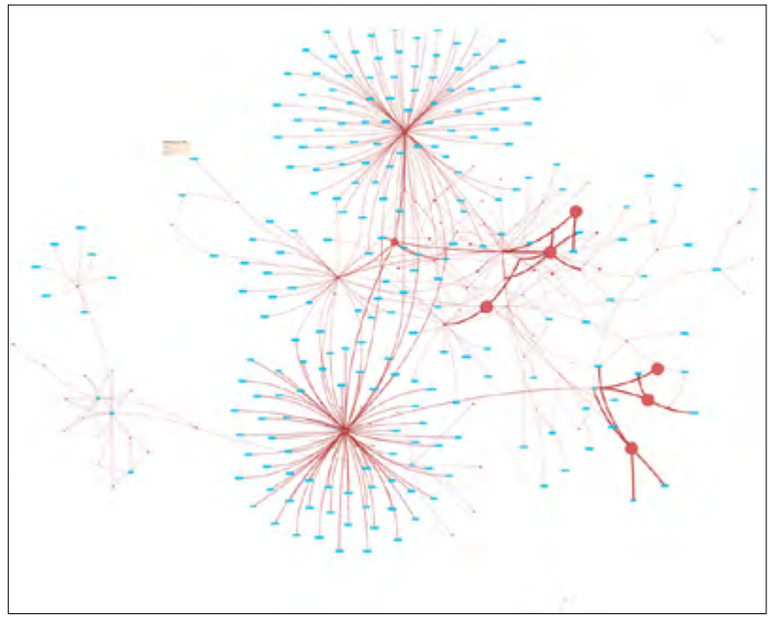
Y es que los CISO y los CSO tienen ante sí dos grandes retos que ninguna empresa puede eludir, porque son la base sobre la que edificar su futuro. En otras palabras, no asumir ambos retos podría suponer la desaparición de una empresa, bien porque cualquier ataque pueda acabar con sus datos o con su reputación, y sin ninguno de los dos elementos se puede vivir, o porque se incumplan las normativas, lo que arriesga a las empresas a multas, en algunos casos,

millonarias, que pueden poner en riesgo su porvenir.

Pero vayamos por partes. El primero de los retos a los que tienen que hacer frente las empresas es el de la explosión de tecnología en las redes corporativas, con más dispositivos, diferentes formatos, diferentes sistemas operativos, diferentes formas de conexión, diferentes lugares, diferentes objetivos... y eso sin tener en cuenta la que se le viene encima a los administradores de las redes con el despliegue masivo de dispositivos con IoT, donde convivirán dispositivos muy inteligentes y autónomos con otros "tontos" que no tengan ni la posibilidad de securizarse a sí mismos.



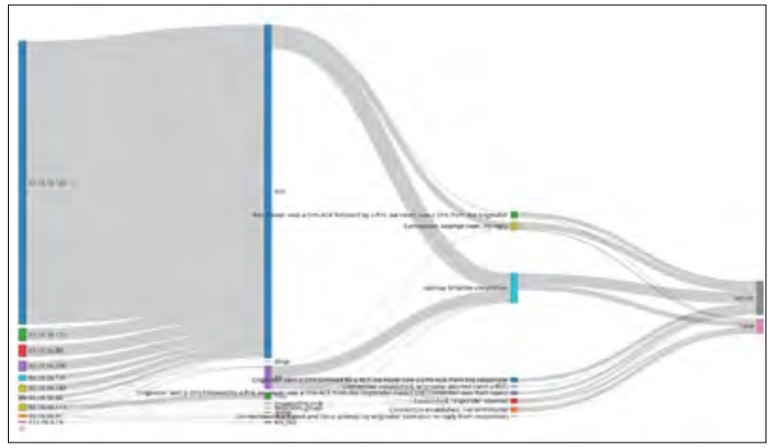
La visibilidad, desde diversos puntos de vista, es fundamental para la seguridad de nueva generación que necesitan las empresas



Las empresas tienen que cambiar su forma de entender y de enfrentarse a la seguridad, porque lo que ha funcionado durante muchos años, como ha sido la seguridad perimetral, ha dejado de tener sentido. Durante años, la propuesta más efectiva para la seguridad era defender el perímetro, y muchos proveedores conectaban esta idea con la imagen de un castillo y un foso. No es que se haya quedado tan anticuado con la imagen, pero el acercamiento a la seguridad desde esta idea ha dejado de ser efectivo, entre otras cosas porque el perímetro, como tal, ha desaparecido. Porque, ¿dónde acaba ahora la red de la empresa? Antes, los usuarios se conectaban por cable a los recursos de red de las compañías. Ahora lo hacen en movilidad mediante 4G, WiFi o VPN desde cualquier lugar, con dispositivos que no siempre han sido proporcionados por la propia compañía ni, en algunos casos, aprobados por el departamento de TI. Además, la empresa está conectada con sus proveedores, y, sobre todo, sus clientes, que quieren que la empresa les atienda siempre y desde donde ellos lo precisen, accediendo en muchos casos a datos muy sensibles para la propia empresa.

Por tanto, el perímetro conocido es una ilusión que no permite servir de base sobre la que desarrollar la red, de ahí que sea necesario buscar otra alternativa.

El segundo gran reto a los que tiene que enfrentarse la empresa, en lo que a la seguridad se refiere, es el cumplimiento de normativas y leyes, tanto internacionales, como pueda ser el caso de GRPD, como por la legislación nacional. El cumplimiento de normativas es algo que no se puede ignorar, y las empresas deben asegurarse de que se cumplen todas y cada una de las normativas de aplicación en la empresa.



NUEVA APROXIMACIÓN A LA SEGURIDAD

Como ya hemos comentado, las empresas deben pensar en cómo diseñar e implemen-

tar la seguridad, de forma que den respuesta a los retos que se les imponen en este momento. Y si algo es necesario tanto para securizar esta red creciente como para el cumplimiento de normativas es la visibilidad de todo lo que está conectado a la red, lo que permite a los responsables de esta seguridad establecer la trazabilidad de todos los accesos a la red.

Por tanto, esta visibilidad puede verse como un primer paso de la seguridad, porque hay que empezar por conocer y entender todo lo que está conectado, tener el máximo información para, sobre esto, ir desarrollando otras capas de la seguridad, como las políticas de control.

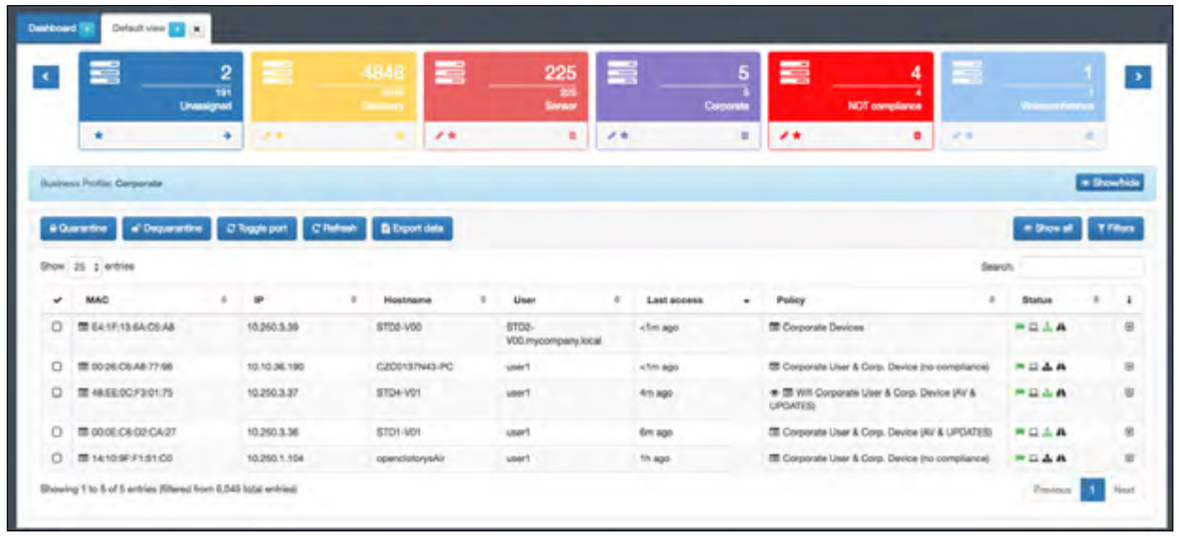
Porque, como indicábamos, el paradigma de seguridad perimetral ha cambiado, y encontramos muchas cosas conectadas dentro y fuera del perímetro. Hay que cambiar la forma de entender la seguridad, que debe verse desde cualquier dispositivo que se conecta a la red.

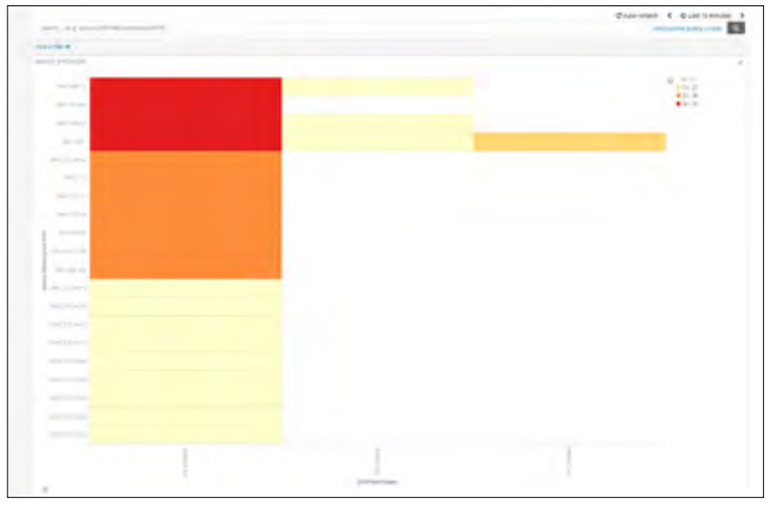
Y si ahora son muchos los dispositivos en la red, ¿qué pasará con el despliegue real de Internet de las Cosas? En el desarrollo de IoT hay dispositivos de todo tipo, y muchos de ellos no tienen capacidad para incorporar una solución de seguridad tradicional, como un antivirus o un antimalware,, con lo que hay que pensar en otras formas de asegurar IoT, y una de las propuestas está precisamente ahí, en la conexión. Cuando un dispositivo intenta conectar hay que anali-

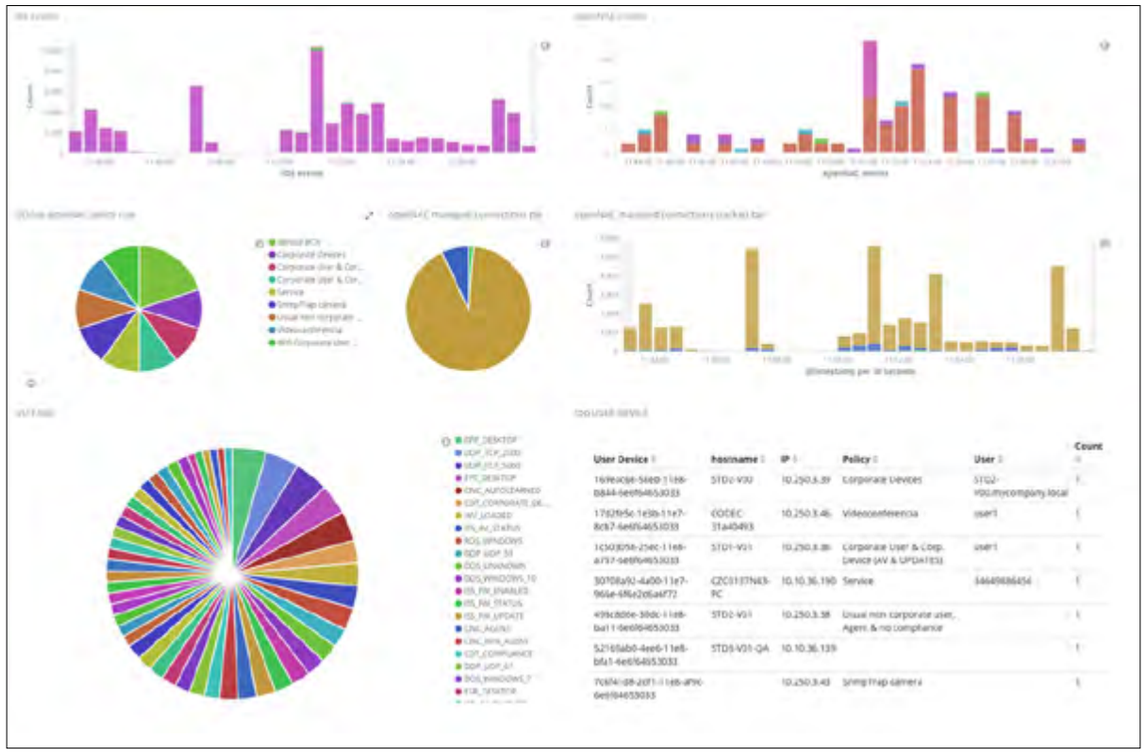
El control sobre los activos es uno de los elementos clave para hacer frente a las amenazas

LA SEGURIDAD SEGÚN OPENCLOUD FACTORY

VISIBILIDAD, CONTROL Y MODULARIDAD: SEGURIDAD DE NUEVA GENERACIÓN







Control sobre todos los elementos de la red, clave en la seguridad

zar el dispositivo y la conexión y determinar el nivel de seguridad adecuada o el área de red a la que pueden conectarse, en función del propio dispositivo y su naturaleza.

TODO LO QUE ESTÁ CONECTADO CUENTA

Las empresas han estado en jaque durante años; el trabajo a distancia, el número cada vez mayor de proveedores/ colaboradores de servicios, BYOD, la implementación de tecnologías de vanguardia y el mantenimiento de soluciones heredadas en productos electrónicos heterogéneos han sido parte de la experiencia cotidiana en la lucha contra incendios para garantizar un panorama de amenazas cada vez mayor. Sin embargo, en 2018 IoT ha empujado a los equipos de operaciones de red y seguridad más allá de un punto sin retorno.

Este 2018 ha marcado un punto de inflexion para IoT dentro de un contexto empresarial. Las organizaciones han pasado de una fase de conceptualización/descubrimento de IoT, que duró algunos años, a una fase de implementación/ejecución para aprovechar las ganancias prometidas de eficiencias de IoT. La mayoría de las empresas que adoptan IoT hoy utilizan métricas e indicadores clave de rendimiento (KPI) que reflejan las mejoras operacionales, la experiencia del cliente, la logística y las ganancias de la cadena de suministro.

Hasta 2018, los principales problemas para las empresas han sido el volumen de dispositivos que se deben proteger y la naturaleza heterogénea/dispersa de las redes, donde cada dispositivo conectado es un punto potencial de ataque o reconocimiento. IoT, además de agregar volumen al problema también ha agregado capas adicionales de complejidad al mismo.

El gasto de la empresa en IoT crecerá inicialmente un 30,7% anual en los próximos 3 años. Todo ese gasto deber ser administrado por una red y un equipo de operaciones de seguridad que no crece al mismo ritmo. Por sorprendente que parezca este crecimiento, no tiene en cuenta que otras cosas, los empleados, invitados y contratistas adoptarán a la red para hacer que su día a día sea más eficiente. Por lo tanto, el total de dispositivos conocidos que se gestionarán no tiene precedentes, pero aún debemos agregar los dispositivos desconocidos (no corporativos).

La mayoría de los dispositivos de IoT son económicos, diseñados especialmente, y de conexión plug and play, todos aspectos positivos desde el punto de vista de la empresa. Sin embargo, esto "faculta" a las unidades/departamentos de negocios para que compren las cosas que necesitan y las conecten directamente a la red para obtener resultados rápidos sin aprovisionarlas primero a través de redes u operaciones de seguridad. Esta falta de "descubrimiento y visibilidad" da como resultado una planificación inadecuada que no está alineada con los objetivos comerciales, lo que genera tiempo perdido, recursos, brechas de seguridad y un mayor riesgo.

¿INSEGUROS POR DISEÑO?

Aunque el artículo 25 del Reglamento General de Protección de Datos establece que toda la protección de datos deber ser por diseño y de manera predeterminada, la realidad es que hasta que se cumplan las reglamentaciones, la métrica clave del éxito para los proveedores de IoT no será la confianza del mercado, sino el tiempo de comercialización. En estos casos, la seguridad es un segundo pensamiento en la mayoría de los casos.

Incluso si los fabricantes cuentan con cierta conciencia de seguridad, la mayoría de los dispositivos IoT son livianos y no tienen la capacidad de instalar y mantener controles de seguridad estándar, como soluciones antimalware, o no pueden escanearse de forma remota, convirtiéndolos en un objetivo fácil para los agentes de malware, abriendo

nuevas rutas de ataque en los entornos de red/IoT.

NO TODAS LAS COSAS SON IGUALES EN IOT

Algunos dispositivos IoT son "terminales brutos" en el sentido de que no procesan datos importantes y, por lo general, están limitados por los recursos. La mayoría tiene un procesamiento y memoria limitados para ayudar a los agentes. En el otro extremo del espectro, algunos dispositivos IoT tienen una increíble potencia de procesamiento que puede aprovecharse malignamente y, lo que es más preocupante, es que procesan datos confidenciales (información de identificación personal, datos de categorías especiales), además de poder cambiar los estados físicos de sus entornos. Esto se ve claramente en el sector de la Salud, donde los datos procesados son fundamentales y la posibilidad de cambiar los estados físicos es literalmente mortal.

EL PRECIO DE LA GLOBALIZACIÓN

Junto con todo lo anterior, el tsunami de IoT, los nuevos colaboradores y los módulos de trabajo, los entornos heterogéneos se combinan con el efecto global, y es que debido a los objetivos de eficiencias corporativas, las organizaciones necesitan administrar oficinas más remotas a través de divisiones geográficas mayores, integrar nuevas compañías mediante adquisiciones/fusiones lo más rápido posible, todo con una debida diligencia y seguridad.

INCREMENTO DE LA VISIBILIDAD

En general, los tiempos de detección, según el Trustwave Global Security Report, han disminuido, debido a la tecnología de seguridad de vanguardia. Sin embargo, los tiempos de respuesta a los ataques aumentan debido, en parte, a los falsos positivos y la complejidad de este nuevo paisaje en expansión conocido y desconocido. Para agravar el problema, el impacto de los ataques, tanto desde un punto de vista económico como de reputación, aumenta a medida que los ataques se han convertido en "ataques a gran escala, multi vector y mega ataques" (informe de ataques de la Generación V, Checkpoint).

Los siguientes controladores para aumentar la visibilidad de las soluciones de IoT también se aplican a todos los activos de la empresa en la mayoría de los casos. El problema de base es común: no se puede controlar, administrar o asegurar lo que no puede ver. La visibilidad es el pre-requisito para la seguridad.

❖ **Presión de regulación y auditoría:** algunos auditores requieren que una organización brinde visibilidad y control sobre todos los dispositivos que están conectados a la red corporativa principal.

En Gartner's Guide to Network Access and Control 2017, Gartner señaló que las consultas de los clientes mostraron una gran demanda de respuesta a los comentarios de los auditores sobre la falta de visibilidad de los dispositivos

❖ **Respuesta y recuperación (Regulaciones):** cuando responden a violaciones de seguridad, las organizaciones necesitan responder y recuperarse rápidamente, tanto desde un punto de vista técnico como desde un punto de vista reputacional. Por la misma razón, cuanto mayor sea la información disponible sobre todos los activos, mejor (por ejemplo, nombre del dispositivo, tipo, ubicación, es un activo crítico...).

El Artículo 33 de la GDRP establece claramente: "medidas tomadas o propuestas a tomar por el controlador para abordar la violación de datos personales, incluidas, cuando corresponda, medidas para mitigar sus posibles efectos adversos".

❖ **Programas BYOD:** BYOD requieren visibilidad y cumplimiento de políticas para garantizar que el empleado no quiera o quiera exponer a las corporaciones a un riesgo mayor.

❖ **Autenticación:** para permitir que la autenticación basada en la red administre qué dispositivos pueden obtener acceso a la red, primero se debe lograr una visibilidad del 100% en todas las capas de acceso (cable, Wi-Fi y VPN).

FRENTE AL PROBLEMA... LA SOLUCIÓN

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. Frente a esto, Opencloud Factory pone sobre la mesa la solución openNAC Enterprise, que, sin importar el tipo de dispositivo y cómo se conecta, automáticamente descubrirá y categorizará todos los activos de su red corporativa.

A través de la visibilidad y control centralizado que aporta openNAC Enterprise, la empresa 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.

Una vez conseguida la visibilidad e información sobre cada conexión (usuario / dis-

CASO DE ÉXITO:
OPECLOUD FACTORY UNIVERSIDAD DE BARCELONA

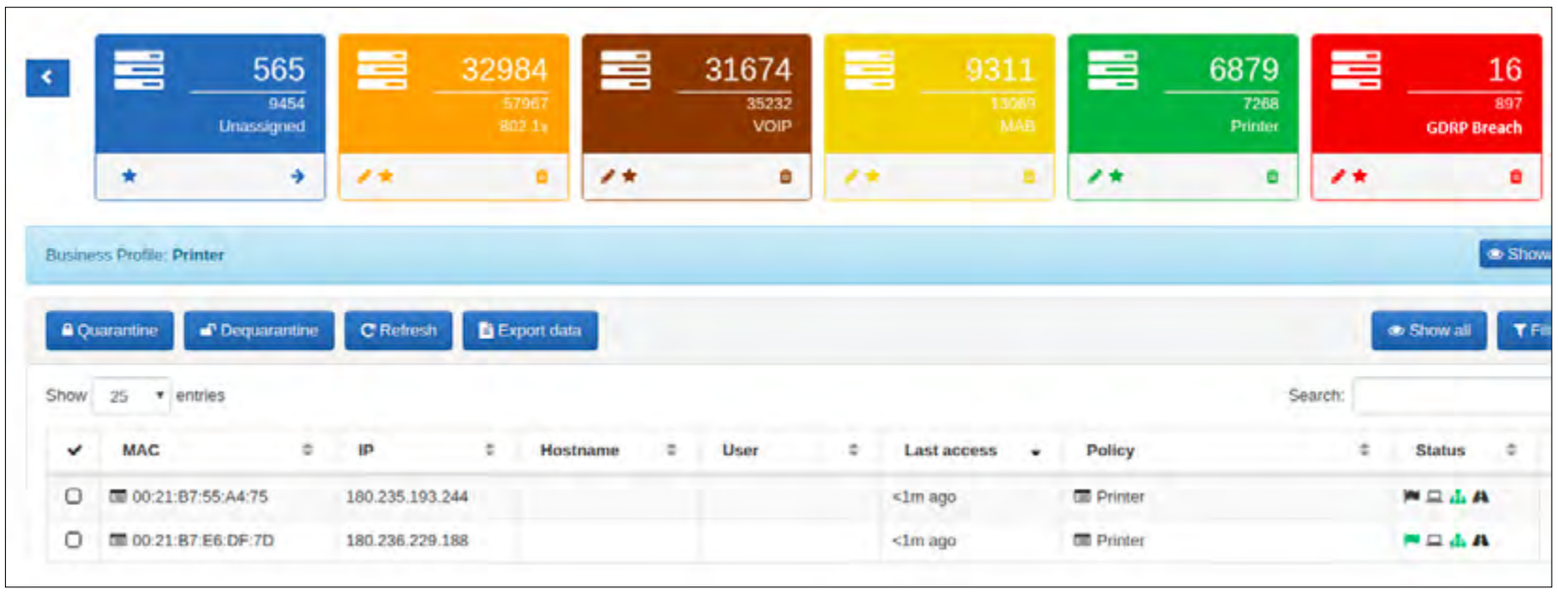
positivo), la solución le proporciona un punto único y central donde puede definir y aplicar políticas de acceso, adaptadas a las necesidades de la organización, y los accesos correspondientes para todos los activos conectados y que intenten conectar. La organización puede, de manera automática, permitir, denegar y limitar todos los accesos (cable, wi-fi y VPN) basándose en la lógica del negocio con una trazabilidad 100% de lo conectado; desde qué dispositivo, con qué credenciales, a que segmento de la red, durante cuánto tiempo ..etc.

Con la misma facilidad la organización puede aplicar una política nueva sobre dispositivos ya conectados para dar respuesta en tiempo real a una incidencia; por ejemplo, ante una brecha de seguridad una organización podrá querer aislar todos los dispositivos afectados que tengan datos personales para responder ante el Artículo 33 del GDPR. La política se aplicará en tiempo real y podrá segmentar los equipos en cuestión y hacerlos un seguimiento desde un *dashboard*.

UNA SOLUCIÓN MODULAR QUE RESPONDE A TUS NECESIDADES HOY Y MAÑANA

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, y 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 una solución que ofrece la seguridad por módulos, proporcionando una seguridad que se adapta a la situación actual, aportando resultados en menos tiempo y con menos esfuerzo. La modularidad de la solución podría incrementarse a medida que crece la complejidad de la propia empresa. ■



MÁS INFORMACIÓN

- Opencloud Factory
- El CISO ante la problemática de la seguridad en su empresa
- Opencloud Factory
- Casos de éxito
- Construcción de un entorno seguro

Principales beneficios de openNAC Enterprise

❖ VISIBILIDAD
➔ Inventario 100% de dispositivos / things, infraestructura y usuarios.
➔ Visibilidad continua automática en la conexión.
➔ Etiquetar activos críticos (GDPR…) 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.

❖ SEGMENTACION 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
➔ Cumplimiento de seguridad del EP con las políticas corporativas / mandatos regulatorios.
➔ Definir y aplicar políticas de seguridad para EP.
➔ Descubrir EP y garantizar el cumplimiento con la política de manera automática.

❖ BOYD SEGURA
➔ Única identidad corporativa
➔ Controlar y rastrear accesos a la red

❖ CONTROL DE ACCESOS DE INVITADOS
➔ Aislamiento automático de la red
➔ Reconfiguración de accesos.

❖ DIFERENTES DESPLIEGUES
➔ Desde la nube:
La implementación en la nube no requiere infraestructura o mantenimiento
➔ On premise: VM son premise no require HW

❖ OTROS VALORES
➔ Escalado horizontal
➔ Entorno multivendor amigable
➔ Adaptable a la infraestructura de red de la empresa