



OpenNAC Enterprise / EMMA & NGFW

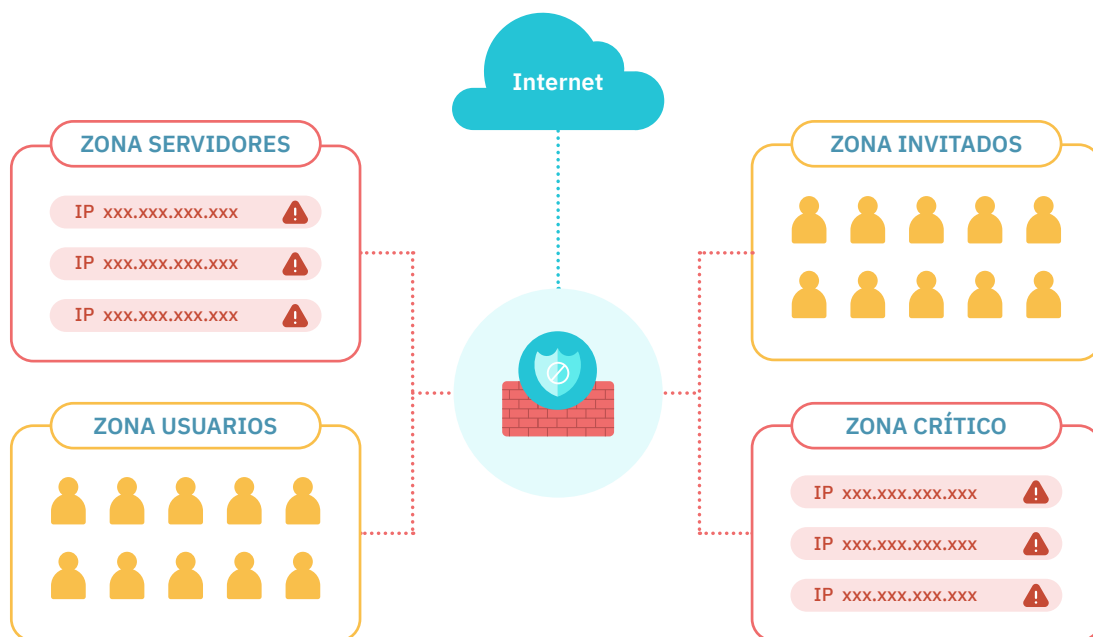
Ampliando el valor del NGFW
con contexto de riesgo

1. Problemática. NGFW Seguridad Perimetral

NGFW Plug-in

OFF

Muchos progresos con NGFW pero falta contexto para fiar o no fiar.



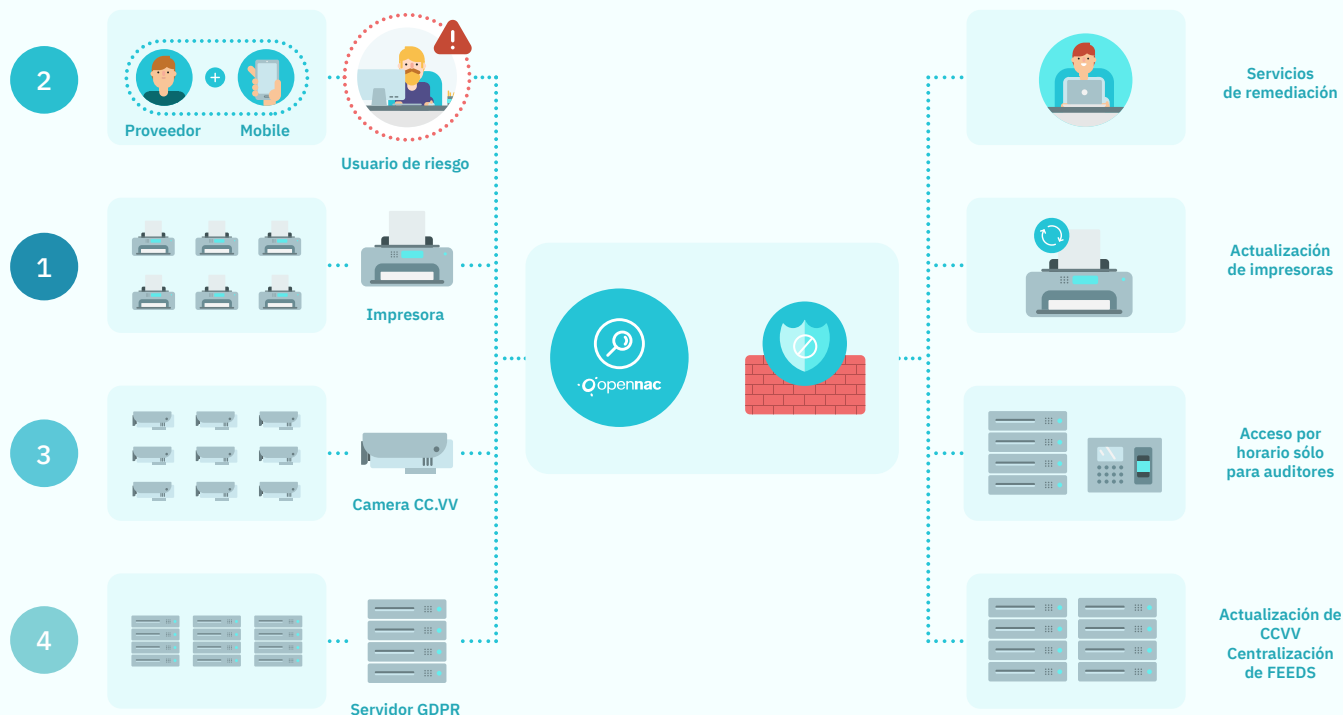
NGFW con funciones de seguridad perimetral, un paradigma de seguridad obsoleto, fiar de dentro y no de fuera. Es necesario cambiar a un enfoque Zero Trust

- Su objetivo principal es la conectividad.
- Conexión / acceso estáticas (IPs – usuarios).
 - Aplicación de política (Cambios) en horarios de producción – Riesgo.
 - Coste de oportunidad (reglas a nivel de aplicación).
 - Podría obtener mucho más valor con poco esfuerzo (sacando más provecho de lo invertido).
 - Explotar más la infraestructura actual.
- Riesgos Internos sin gestionar – No Zero Trust

2. La Solución. Integración con NGFW - NGFW Zero Trust. Las fuentes de riesgo no son estáticas

NGFW Plug-in

ON



Beneficios. Ampliando el valor del NGFW con contexto de riesgo.

1

Implementar seguridad, accesos dinámicos, basado en el **riesgo** de la conexión (Printer, IoT, CCVV..)

2

Sacar **mayor provecho** de la inversión - infraestructura actual.

3

Adaptar a la infraestructura actual y del futuro (IPv6...etc.); **Tecnología Agnóstica.**

4

Automatizar tareas de segmentación y control.

Ayuda al establecimiento del principio de mínimo privilegio y cumplimiento de estándares de buenas prácticas, ENS, ISO 27001, NIST.

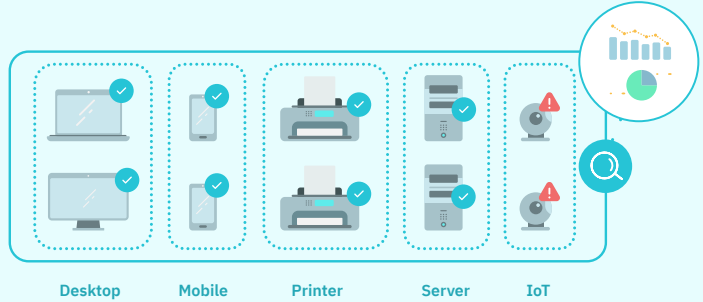
3. Casos de uso.

Asignación de reglas de acceso en base a:

1

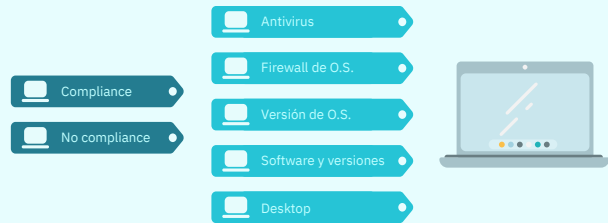
Tipología y/o perfil de riesgo de dispositivo (pasivo).

Los dispositivos conectados a la red serán cualificados dependiendo su tipo y/o riesgo asociado.



2

Evaluación de Postura de Seguridad del dispositivo (activo)



3

Destino únicamente permitido para auditoría en horario x de la mañana el último día de cada mes.

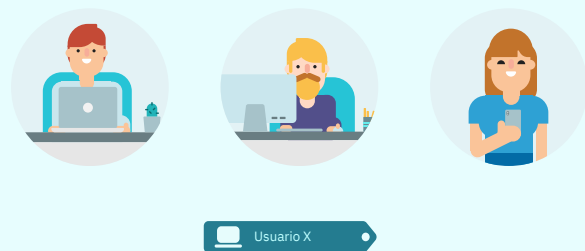


4

Identidad, grupo, perfil de usuario.

Cada usuario tendrá únicamente los accesos correspondientes con su rol en la compañía:

- Proveedores
- Privileged accounts
- Departamentos con menor requisitos de acceso



4. Valor contrastado en el mercado.

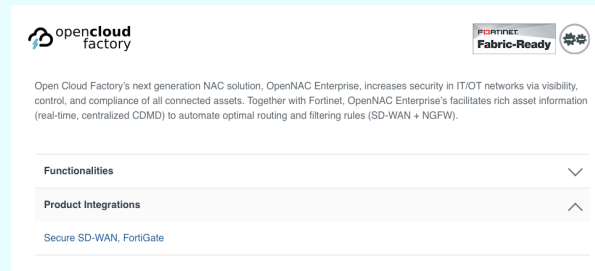
NGFW Plug-in

ON

Integración con los NGFWs más importantes del mercado (Palo Alto y Fortinet):

FORTINET

paloalto
NETWORKS



Integraciones contrastadas con clientes de referencia al nivel mundial:



Se trataba de un ambiente donde tenían visibilidad limitada en las oficinas remotas, desconocían cuántos y cuáles dispositivos y usuarios se conectaban en sus oficinas para aplicar la regla correspondiente al riesgo.

Necesitaban una solución con el mínimo impacto en las operaciones de negocio, se trataban de ambientes muy sensibles que tenían que ser intervenidos sin detener la producción.

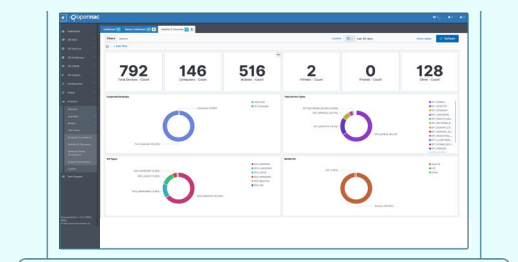


5. Valor añadido. Beneficios colaterales

NGFW Plug-in

ON

Al desplegar la integración con el NGFW la empresa puede aprovechar de mucha más funcionalidad out of the box.



- **Automatiza** el descubrimiento e inventariado del 100% de los dispositivos conectados a la red corporativa (Cuantificación de Activos de red).
 - Nuevos dispositivos diarios
- **Perfila y clasifica** automáticamente todos los dispositivos conectados a la red (Cualificación de Activos), asignando tipología a cada conexión (móvil, desktop, cámara, etc), base del establecimiento de políticas de acceso para dispositivos.

Certified by



Collaborating with



Published



Trusted by



Nuestras oficinas



SPAIN



BRAZIL



MEXICO



USA

916 14 53 22 opencloudfactory.com/contacto