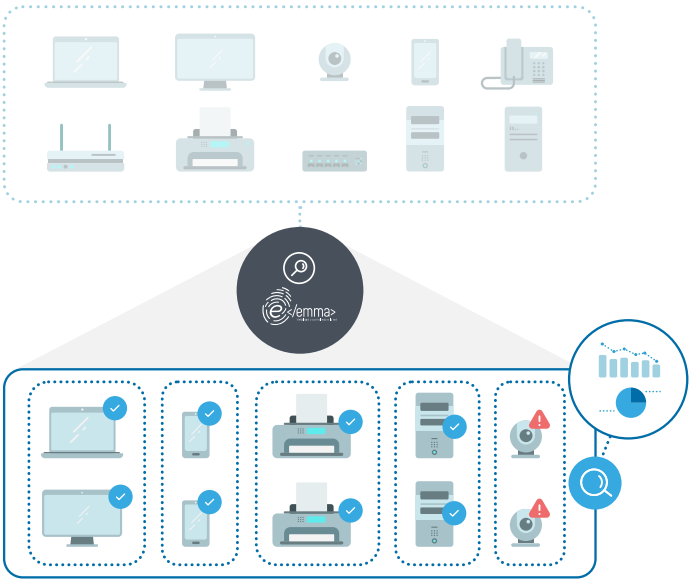
El conocimiento de la **superficie de exposición** supone conocer los diferentes puntos donde un usuario no autorizado puede intentar ingresar o extraer datos; es un punto clave para el establecimiento de controles e iniciativas de seguridad. Establecer la visibilidad de red es imperativo para la gestión del riesgo en entornos corporativos. No se puede proteger lo que no se ve.



El problema

Cada conexión que se realiza en la red representa un punto donde un usuario no autorizado puede intentar ingresar o extraer datos.

- Gestionar el riesgo asociados a los dispositivos en la red requiere el conocimiento del activo que hay detrás de cada conexión.
- Mantener un inventario actualizado de todos los activos de red, no puede ser una tarea manual, es una tarea compleja que requiere herramientas de automatización.
- No es posible establecer mecanismos de gestión de riesgo si no se tiene un conocimiento de la superficie de exposición.
- Identificar los activos críticos de la red es la tarea inicial para su protección.

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

Se estima que a cada persona en un ambiente corporativo se le vinculen por lo menos tres dispositivos conectados a la red, teniendo en cuenta dispositivos como computadoras, móviles, teléfonos IP, impresoras, cámaras, relojes, entre otros. Cada dispositivo conectado a la red supone cierto valor de riesgo, la primera tarea para gestionar el riesgo asociado a un dispositivo es identificar el dispositivo. Descubrir, cuantificar y cualificar el 100% de los activos a la red es el reto que debe afrontar las compañías para realizar una adecuada gestión de riesgo.

Conocer la superficie de exposición

- La visibilidad es el punto de partida para establecer controles de seguridad, descubrir las conexiones en redes cableadas, Wi-Fi y VPN permitirá el establecimiento de iniciativas de seguridad para cada entorno.

Establecer una estrategia Zero Trust

- No se puede otorgar confianza a ninguna conexión realizada en la red, para ello es necesario descubrir todas las conexiones realizadas en la red y conocer el activo asociado, cada dispositivo conectado en la red supone un punto de riesgo a gestionar.

La Solución:
Visibilidad

Visibilidad es un módulo dentro de **EMMA** que descubre, cuantifica y cualifica los activos conectados a la red corporativa, permite conocer los flujos de comunicación en la red, de esta manera ayuda a determinar y gestionar la superficie de ataque en redes corporativas.

Garantiza un punto de partida para establecer los controles de seguridad, base de la gestión del riesgo asociado a los dispositivos. Facilita la adecuación de estándares y frameworks como **ISO2700x, NIST, ENS etc.**

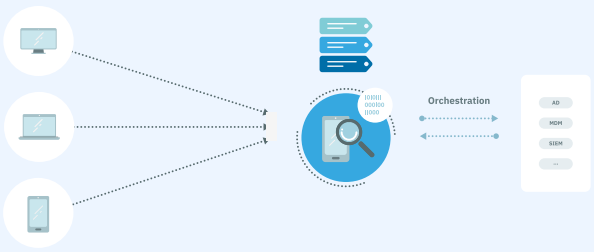
Modos de Visibilidad

Las empresas pueden escoger **la(s) fuente(s) de visibilidad** que desean implementar.

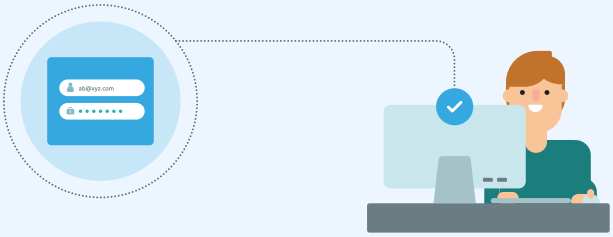
Visibilidad			
Modo	**Dispositivos de Red**	**Sensor**	**Agente**
Opera en:	Capa 1 - 4 	Capa 2 - 7 	S.O 
Información base	IP - MAC		
Mecanismo	802.1x Accounting Events, DHCP Request Events, MAC Table for Switches & Routers, SNMP Traps Events y Custim Reader	El sensor debe conectarse a traves de un port SPAN. Se escucha todo el el trafico que pasa por esta interfaz.	El agente debe instalarse en el End-Point.
Cuantificación de Activos, Discovery	✓	✓	✓
Cualificación de Activos, Profiling	✓	✓	✓
Implementar lógica de Negocio	✓	✓	✓
Análisis de comportamiento de red		✓	
Inventariado de Software y Hardware EP			✓

Puesta en marcha en 4 pasos

1. Descubrimiento:
Establecer la(s) fuente(s) de visibilidad.



3. Definición de Reglas de Negocio:
Crear las políticas para agrupar los activos.



2. Perfilamiento:
Definir las reglas de perfilamiento de activos.

4. Visualizar Resultados:
Obtener valor de toda la información recopilada.

Un ambiente donde detener la producción era algo que no podía pasar. Necesitábamos una tecnología poco intrusiva para empezar a identificar riesgos y gestionarlos.

Testimonio del responsable de infraestructura de uno de nuestros clientes. (Compañía siderúrgica)

Beneficios de Visibilidad

- **Automatiza** el descubrimiento e inventariado del 100% de los dispositivos conectados a la red corporativa **(Cuantificación de Activos de red)**.
- **Perfila y clasifica** automáticamente todos los dispositivos conectados a la red **(Cualificación de Activos)**, asignando tipología a cada conexión (móvil, ordenador, cámara, etc), base del establecimiento de políticas de acceso para dispositivos.
- **Etiqueta y agrupa** los dispositivos conectados en la red **(criticidad de dispositivos, tipología, perfil de riesgo)**. 100% personalizable de acuerdo con el requerimiento de negocio.
- **Muestra el comportamiento de red,** flujos de comunicación, protocolos de red utilizados y estadísticas de comportamiento en **tiempo real**.
- **Facilita la adecuación de estándares y frameworks** como ISO2700x, NIST, ENS etc.

emma
Visibilidad y control sobre la red

emma@ccn-cert.cni.es
www.ccn-cert.cni.es

ccn-cert