AVANSYS
SISTEMAS AVANZADOS INTEGRALES

EDR

EndPoint Detection and Response

Protección avanzada y siempre activa.

AVANSYS
SISTEMAS AVANZADOS INTEGRALES

Un antivirus tradicional, ¡Ya no es suficiente!

En esta nueva era digitalizada en donde las formas de trabajo han migrado al formato remoto y a la nueva normalidad, las empresas necesitan **proteger los dispositivos** de cada colaborador, así como los **entornos de trabajo** de cualquier **ciber amenaza.**

Poderosa herramienta contra
vulnerabilidades cibernéticas

Endpoint Detection and Response: **La evolución de los antivirus tradicionales**

Es una poderosa herramienta que proporciona **monitorización** y **análisis continuo** del EndPoint y la red, **detecta ataques que no son visibles** para un antivirus y además **monitoriza** y **evalúa** todas las actividades de la red.

¡Queremos que tu **empresa esté protegida** frente a cualquier posible incidente de seguridad; amenaza tradicional, aplicación vulnerable o amenaza desconocida! Protégete contra amenazas de **Día Cero, dentro y fuera del perímetro, y protección de Zero Trust (Confianza Cero).**

AVANSYS
SISTEMAS AVANZADOS INTEGRALES

EndPoint

Es Cualquier **dispositivo informático que esté conectado a una red** (Computadora, Laptop, Celular)

EPP
(EndPoint Protection Platform)

Un EPP es un **conjunto de tecnologías de protección de EndPoint.** Es una solución que proporciona **seguridad esencial** para muchos tipos de EndPoints, desde teléfonos inteligentes hasta impresoras. Ofrece un **enfoque mas eficaz** que el que puede otorgar una colección de productos de seguridad aislados.

EDR
(EndPoint Detection and Response)

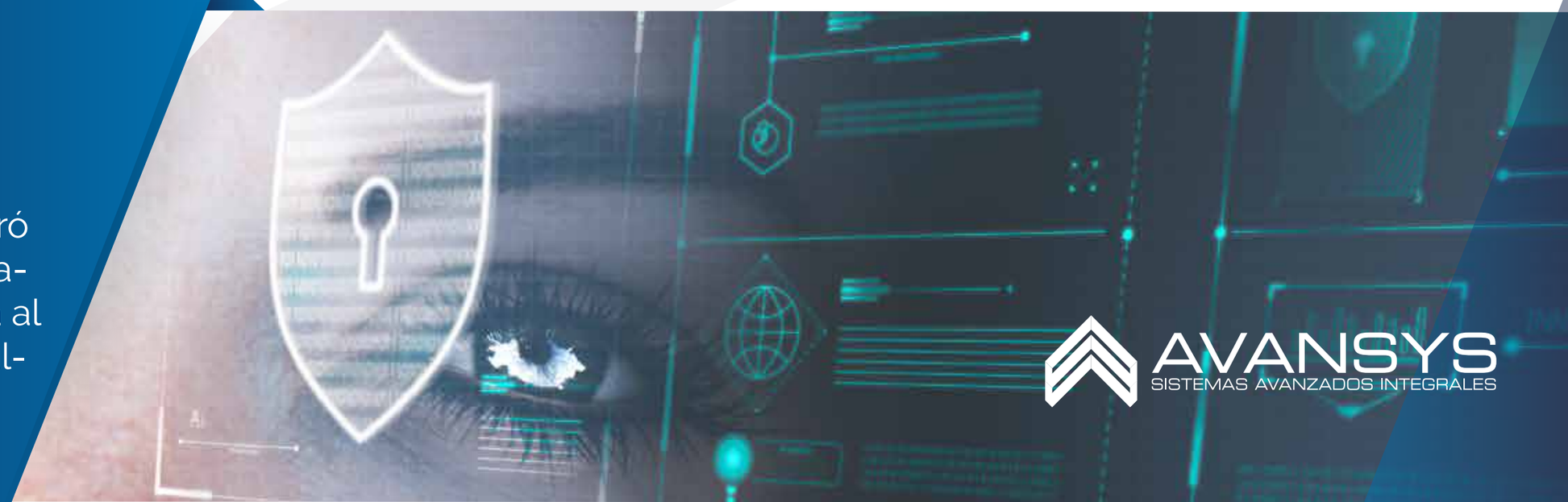
Es una poderosa herramienta que proporciona **monitorización y análisis continuo** del EndPoint y la red, detecta **ataques que no son visibles** para un antivirus y además **monitoriza y evalúa** todas las actividades de la red.

¿Por qué tener un EDR en mi empresa?

¡Sencillo! Te damos 7 razones;

- **Mayor anticipación a los ataques dirigidos:** Con el modelo de prevención (pre-infección) y de detección (post-infección) se **analizan patrones de comportamiento** lo que permite anticipar amenazas.
- **Enfoque Proactivo:** Disminución del tiempo de exposición a incidentes de seguridad gracias a un enfoque proactivo que permite **actuar en cuestión de segundos** o minutos.
- **Visión global:** Proporciona visión global de las amenazas contra los endpoints.
- **Filtrado:** Detecta las **amenazas reales y falsos positivos**, poniendo en revisión cada archivo con aspecto sospechoso y **bloqueando** cualquier contenido malicioso que desee entrar a tu sistema.
- **Bloqueo avanzado de amenazas:** evita las amenazas en el momento en que se detecten, pero también mientras dure el ataque.
- **Buena capacitad de respuesta ante incidentes:** La mejor y más oportuna respuesta ante cualquier tipo de ataques.
- **Protección múltiple:** Tiene la capacidad para poder manejar v**arias amenazas avanzadas al mismo tiempo,** por ejemplo, varios tipos de malware o cualquier otro tipo de amenaza como a**cceso no autorizados o movimientos sospechosos de los datos.**

> “
>
> El reporte ESET Security Report LATAM 2020 mostró que el 69% de las organizaciones en el país presenta al menos un incidente de vulnerabilidad.



AVANSYS
SISTEMAS AVANZADOS INTEGRALES

0%

Nigún dispositivo en modo “lock” ha sido **infectado**

1 TB

Diariamente **analiza, correlaciona y categoriza** más de 1TB de información de todo tipo de ciberataques

3.5 M

Ha **categorizado** más de 3.2 millones de **aplicaciones** hasta ahora

2.3 M

Más de 2.3 millones de **brechas de seguridad** han sido **bloqueadas**.

100%

Ha **detectado** malware en el **100% de los entornos** en los que ha sido instalado, independientemente de las soluciones de seguridad que ya se tenían instaladas

Características

AVANSYS
SISTEMAS AVANZADOS INTEGRALES

Monitoreo de actividad:

Monitoriza la actividad de los EndPoints y realiza una clasificación de los archivos según sean seguros, peligrosos o desconocidos.

Aislamiento de amenaza

Cuando **detecta archivos sospechosos** (desconocidos) en uno de los Endponts, por ejemplo: un **adjunto en un correo**, automáticamente lo mando a un **entorno de pruebas en la nube**, en donde se **ejecutará imitando el comportamiento** que tendría el usuario con él.

Determina si es seguro o peligroso:

Una vez en el entorno de prueba en la nube, el sistema de machine learning observa y aprende del comportamiento de la amenaza. Tras observarlo un tiempo, se podrá determinar si es seguro o peligro.

Bloqueo de amenaza:

Si el archivo se considera peligroso, se bloqueará en todos los EndPoints.

Características

AVANSYS
SISTEMAS AVANZADOS INTEGRALES

Seguridad continua de información:

De ese modo, sin el futuro se detecta de nuevo ese archivo en cualquiera de los endpoints, directamente lo bloqueará impidiendo su ejecución.

Detección:

Utilizan la IA (Inteligencia Artificial) para reducir la tasa de falsos positivos. Los equipos pueden optimizar los recursos clave y centrarse en tareas de TI importantes en lugar de revisar un gran volumen de alteras y falsos positivos. Logra detectar ransomware, malware, botnets y otras amenazas conocidas y desconocidas, accesos no autorizados, ataques sigilosos par robo de datos y más.

Contención:

Permite un bloqueo avanzado de amenazas. No sólo es capaz de detectar rápido nuevas amenazas, sino que puede manejar ataques en directo y protegerte mientras estos se producen.

¡Características que convierten al **EDR** en una herramienta **poderosa y confiable!**

AVANSYS
SISTEMAS AVANZADOS INTEGRALES

Antivirus tradicional

VS

Adaptive defense

	Antivirus tradicional		Adaptive defense
01	Basado de **ficheros de firmas**	VS	Protege contra **todo tipo de amenazas** malware **conocidas** y **desconocidas** y cualquier tipo de ataque
02	Solo detecta malware **conocido**	VS	Un servicio gestionado que continuamente **monitoriza, registra y clasifica el 100%** de los procesos activos
03	Solo notifica cuando descubre algo que sabe es **malicioso**	VS	**Prevención, detección y remediación**
04	Protección **básica**	VS	Información forense detallada, **auditoría de seguridad** y alertas en **tiempo real**
05	No ofrece **información sobre el ataque**	VS	Basado en **inteligencia de comportamiento** (**Big Data + Machine Learning**)
06	Detiene malware cuando entra en el EndPoint pero **no monitoriza su actividad**	VS	**Visibilidad total** de la actividad del EndPoint

AVANSYS
SISTEMAS AVANZADOS INTEGRALES

¡No dejes que el malware acabe con tu empresa!

Protege, aisla y actúa

¡Contrata ya!

¿Te gustaría conocer más información? ¡Contactános!

San Felipe Neri #585
Col. Camino Real, 45040
Zapopan, Jal.

(33) 3125 6832
(33) 1057 0121

info@avansys.com.mx
www.avansys.com.mx