

DESCUBRE EDR, NDR Y XDR



SAÚL RUIZ PLAZA

EL NUEVO JUEGO DEFENSIVO

En los últimos años han aparecido términos como EDR, XDR y NDR en casi cualquier conversación sobre ciberseguridad.

En un mundo en el que el atacante tiene múltiples caminos para entrar, la defensa ya no se limita a un firewall: se trata de observar, entender y responder en tiempo real.



SAÚL RUIZ PLAZA



EL PERÍMETRO YA MURIÓ

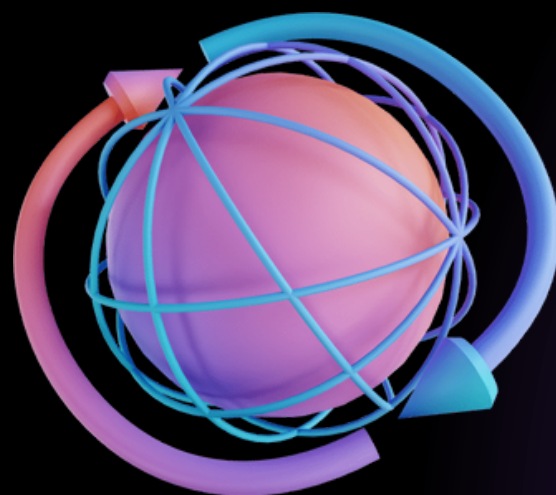
El modelo clásico de seguridad ha quedado obsoleto. El teletrabajo, cloud, accesos remotos y dispositivos personales han revolucionado la seguridad perimetral.

Defender hoy implica contar con telemetría y procesos capaces de identificar comportamientos inusuales en el momento en que ocurren y responder con rapidez, reduciendo así el tiempo en que un atacante permanece dentro de un entorno (dwell time).

Según Google M-Trends 2025, la media de tiempo de detección es de 11 días



SAÚL RUIZ PLAZA



SOLUCIONES EDR EJEMPLOS



**Microsoft Defender
for Endpoint**



CrowdStrike Falcon



SAÚL RUIZ PLAZA



EDR: OJOS EN EL ENDPOINT

ENDPOINT DETECTION AND RESPONSE

Es una tecnología enfocada en los endpoints, como ordenadores y servidores, que recopila telemetría continua del sistema para analizar comportamientos sospechosos que un antivirus tradicional no puede identificar.

No solo detecta amenazas, sino que también permite investigar qué ha ocurrido y responder en tiempo real, aislando equipos o deteniendo procesos maliciosos.



SAÚL RUIZ PLAZA



EDR VS ANTIVIRUS

El antivirus tradicional bloquea amenazas conocidas mediante firmas y reglas, pero tiene poca visibilidad sobre ataques modernos o técnicas fileless.

El EDR, en cambio, asume que un ataque puede ocurrir y se centra en detectar comportamientos sospechosos, investigar y responder en tiempo real.

Lo ideal es usar ambos a la vez, ya que combina prevención con detección avanzada.

Según Techloy, hasta el 79% de los ataques modernos pueden evadir un antivirus tradicional, pero son detectables con EDR.



SAÚL RUIZ PLAZA



NDR: LA RED NO MIENTE

NETWORK DETECTION AND RESPONSE

Analiza el tráfico de red para detectar anomalías, movimientos laterales y comunicaciones sospechosas incluso cuando no hay malware visible en los endpoints.

En muchos casos, las primeras señales de un ataque aparece en el tráfico.



SAÚL RUIZ PLAZA



SOLUCIONES NDR EJEMPLOS

VECTRA®

Vectra AI



Stealthwatch

Cisco Stealthwatch



SAÚL RUIZ PLAZA



EDR, NDR, XDR

¿CÚANDO UTILIZARLOS?

- Usa EDR cuando quieras monitorear endpoints y detectar ransomware, abuso de scripts o escaladas de privilegios.
- Usa NDR para observar la red y detectar movimientos sospechosos, túneles o exfiltración de datos.
- Usa XDR cuando necesites una visión completa que conecte endpoints, red, identidad y cloud, detectando ataques que cruzan capas y fases.



SAÚL RUIZ PLAZA



XDR: LA VISIÓN COMPLETA

EXTENDED DETECTION AND RESPONSE

Combina lo mejor de EDR y NDR: recoge visibilidad profunda de endpoints y tráfico de red, correlacionando eventos para detectar ataques complejos en varias fases. Convierte señales aisladas en contexto accionable, permitiendo priorizar y automatizar la respuesta de forma más rápida y efectiva.

Según Cisco, XDR puede reducir hasta un 30% el tiempo de investigación en SOC's.



SAÚL RUIZ PLAZA



SOLUCIONES XDR EJEMPLOS



**Trend Micro Vision
One**



**Palo Alto Cortex
XDR**



SAÚL RUIZ PLAZA



EDR, NDR Y XDR

BENEFICIOS

Estas tecnologías, cuando se usan juntas, aprovechan la IA y el machine learning para transformar grandes volúmenes de alertas en información accionable, ayudando al SOC y al SIEM a priorizar los incidentes más críticos y a reducir el ruido de falsos positivos.

Los equipos de seguridad pueden responder más rápido y de manera coordinada, automatizando acciones repetitivas sin perder control y acelerando significativamente la investigación y remediación de incidentes.



SAÚL RUIZ PLAZA



EDR, NDR Y XDR

PRECAUCIONES

Si se despliegan sin planificación ni configuración adecuados, pueden generar alertas falsas y saturar al equipo, lo que reduce la efectividad de la estrategia de ciberseguridad.

Además, depender únicamente de la automatización sin supervisión humana puede provocar errores en la respuesta a incidentes.



SAÚL RUIZ PLAZA



**SÍGUEME PARA MÁS
CONTENIDO**

