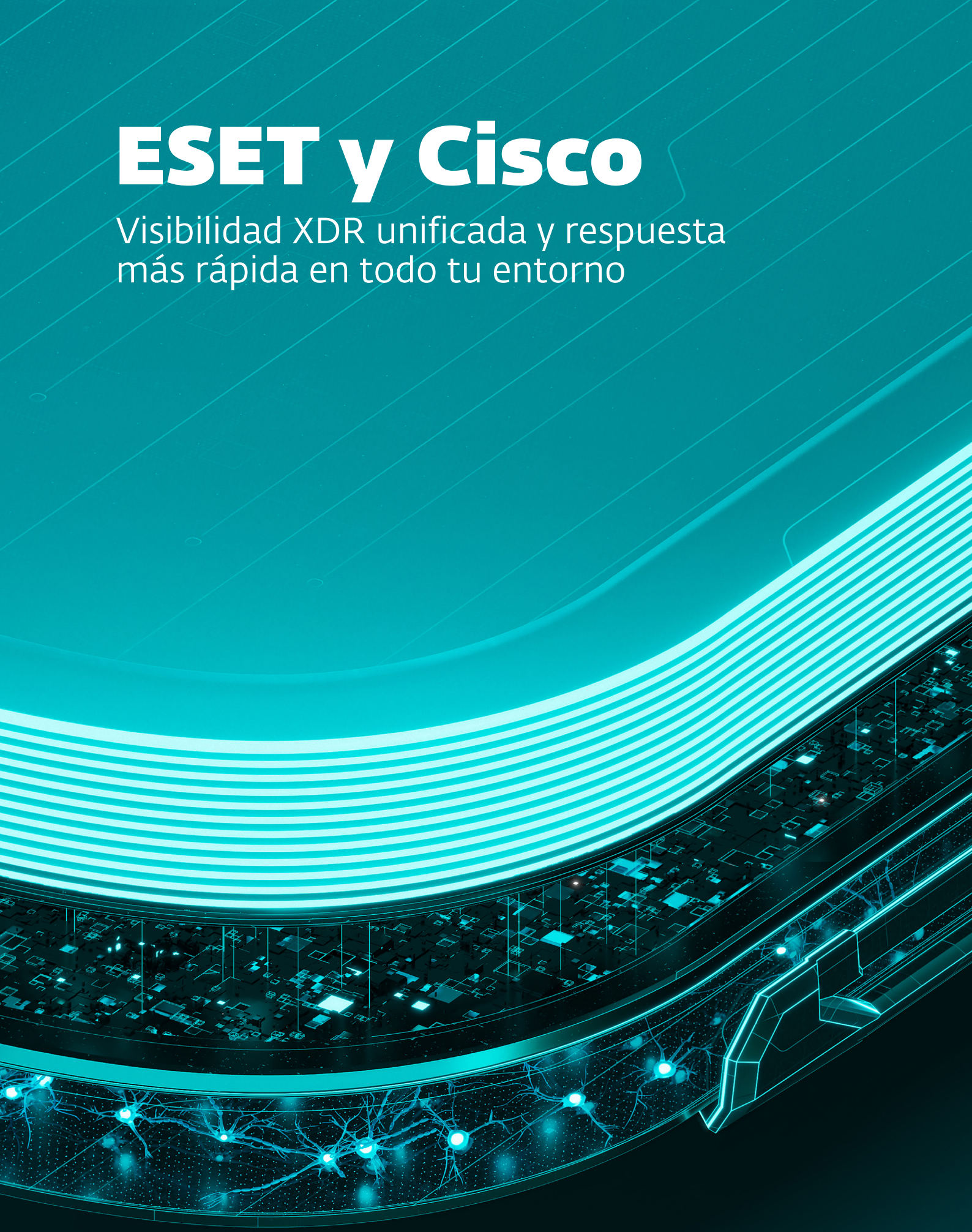
# ESET y Cisco

## Visibilidad XDR unificada y respuesta más rápida en todo tu entorno



Cybersecurity
Progress. Protected.

RESUMEN DE LA SOLUCIÓN

# Inteligencia consolidada de endpoint y redes para tomar decisiones más rápidas y seguras

Los equipos de seguridad suelen tener dificultades al tener que gestionar múltiples consolas, fuentes de datos y herramientas. Cuando las detecciones de endpoint se encuentran en un lugar y la telemetría de red en otro, las investigaciones se ralentizan y las amenazas pueden pasar desapercibidas. Las empresas necesitan una forma de unir estos mundos sin añadir complejidad.

La integración de ESET con Cisco XDR une estos mundos a la perfección. La integración envía los indicadores endpoint de ESET PROTECT a Cisco XDR, lo que proporciona a tu SOC una visión unificada de la actividad de endpoint, la red y la nube, de modo que los analistas pueden responder con mayor rapidez y confianza.

## VENTAJAS PRINCIPALES

### MEJOR RENDIMIENTO DE LAS INVERSIONES EXISTENTES

Aumenta el valor tanto de ESET como de Cisco conectándolos, no sustituyéndolos. La integración te permite aprovechar tus herramientas y procesos actuales, en lugar de empezar desde cero.

### MENOS SILOS, OPERACIONES MÁS SENCILLAS

Salva la brecha entre los flujos de trabajo de endpoint y XDR con flujos de datos automatizados, contexto coherente y vistas compartidas para investigaciones más eficientes.

### VISIBILIDAD UNIFICADA

Observa los indicadores endpoint de ESET junto con la telemetría de red, nube e identidad de Cisco XDR para que los analistas puedan ver el historial completo de un ataque en un solo lugar.

### DETECCIÓN Y RESPUESTA ACELERADAS

La ingestión y la correlación automatizadas reducen el esfuerzo manual y ayudan a tu SOC a pasar de la detección a la contención en menos tiempo.

# CARACTERÍSTICAS PRINCIPALES

### MAPEO NATIVO DE CISCO CTIM

Los eventos de ESET se transforman en «Sightings» y «Judgments» de CTIM de Cisco, lo que garantiza que los datos lleguen en un formato que Cisco XDR comprenda, correlacione y pueda actuar de inmediato.

### VISIBILIDAD INTEGRAL Y COHERENTE

Al alinear la inteligencia de los endpoint de ESET con la telemetría de red y en la nube de Cisco, los analistas obtienen una visión clara del comportamiento de los ciberdelincuentes en todo el entorno.

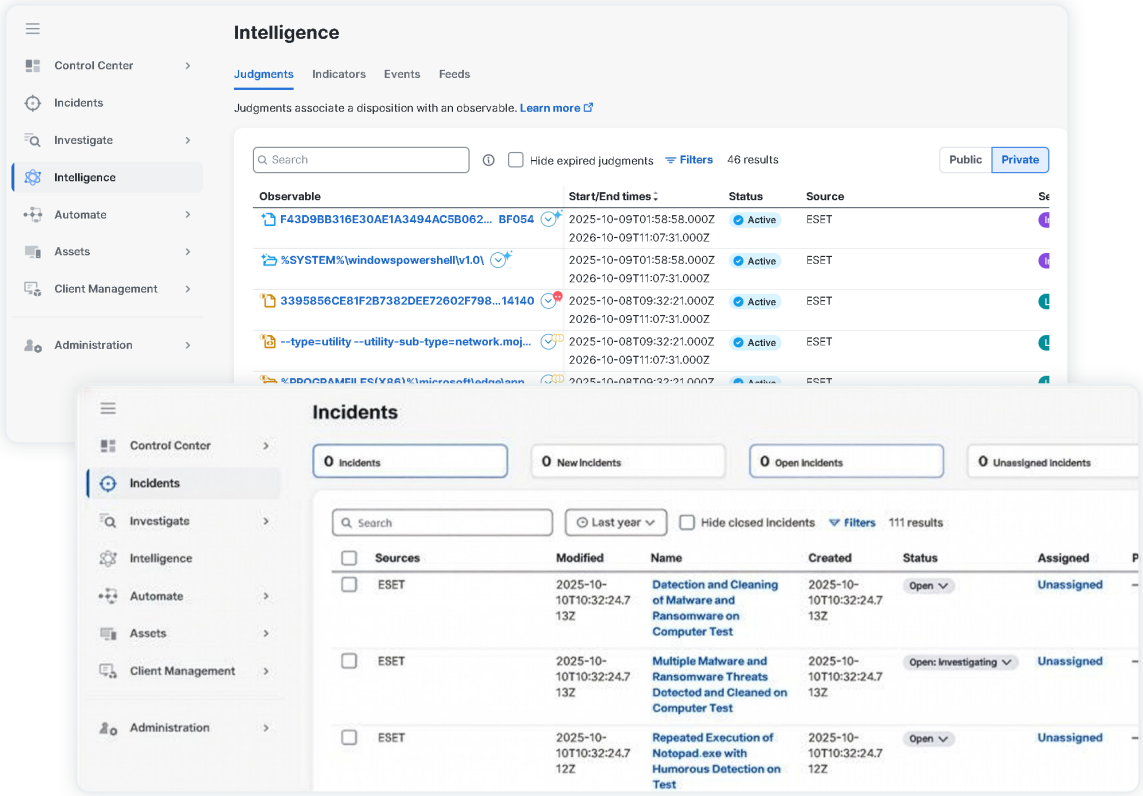
### FLUJO DE DATOS AUTOMATIZADO DE LOS ENDPOINT A XDR

La integración extrae continuamente los datos de detección e incidentes de ESET PROTECT a través de ESET Connect y los envía a Cisco XDR. Se acabaron las exportaciones manuales y el intercambio de datos ad hoc.

# CÓMO FUNCIONA

La integración de ESET y Cisco utiliza la API ESET Connect para extraer datos relevantes de detección e incidentes de ESET PROTECT. Estos datos se normalizan y se convierten al formato CTIM de Cisco como «Sightings» (avistamientos) y «Judgments» (juicios). Una aplicación basada en Docker, implementada en tu entorno, sondea periódicamente ESET y reenvía estos eventos transformados a Cisco XDR.

Dentro de Cisco XDR, esta inteligencia de endpoint se correlaciona automáticamente con la telemetría de la red, el cortafuegos, la identidad y la nube. Los analistas obtienen una línea de tiempo única y consolidada de eventos que abarca tanto los endpoints protegidos por ESET como la infraestructura observada por Cisco, lo que hace que el análisis de la raíz de la causa y la coordinación de la respuesta sean más rápidos y fiables.



# Ejemplo de caso de uso

1. ESET detecta un proceso sospechoso en un endpoint (por ejemplo, un proceso que se genera a partir de un padre inusual o que se comunica con un dominio malicioso conocido).

2. La integración reenvía esta detección a Cisco XDR, donde se correlaciona con los registros del cortafuegos y las anomalías de la red que muestran que el mismo host se comunica con IP externas peligrosas.

3. Desde la consola de Cisco XDR, el SOC puede pivotar hacia el contexto completo del incidente y activar una respuesta automatizada: aislar el endpoint afectado a través de ESET, bloquear los dominios maliciosos en los controles de seguridad de Cisco y actualizar las políticas para la prevención de comportamientos similares en el futuro.

El resultado es una contención más rápida, una reducción de los gastos generales de investigación manual y una aplicación más coherente en todo el entorno.

## Acerca de ESET

**DEFENSA PROACTIVA. MINIMIZA LOS RIESGOS CON LA PREVENCIÓN.**

Disfruta de la mejor protección de su clase gracias a la inteligencia global sobre amenazas cibernéticas de ESET, recopilada y analizada durante más de 30 años, que impulsa nuestra amplia red de I+D dirigida por investigadores reconocidos en la industria. ESET PROTECT, nuestra plataforma de ciberseguridad XDR basada en la nube, combina capacidades de prevención, detección y búsqueda proactiva de amenazas de última generación. ESET protege tu negocio para que puedas aprovechar todo el potencial de la tecnología.

## Acerca de Cisco

Cisco es el líder tecnológico mundial que está revolucionando la forma en que las empresas se conectan y protegen en la era de la IA. Durante más de 40 años, Cisco ha conectado el mundo de forma segura. Con sus soluciones y servicios líderes en el sector basados en IA, Cisco permite a sus clientes, distribuidores y comunidades impulsar la innovación, mejorar la productividad y reforzar la resiliencia digital. Con un propósito fundamental, Cisco mantiene su compromiso de crear un futuro más conectado e inclusivo para todos.