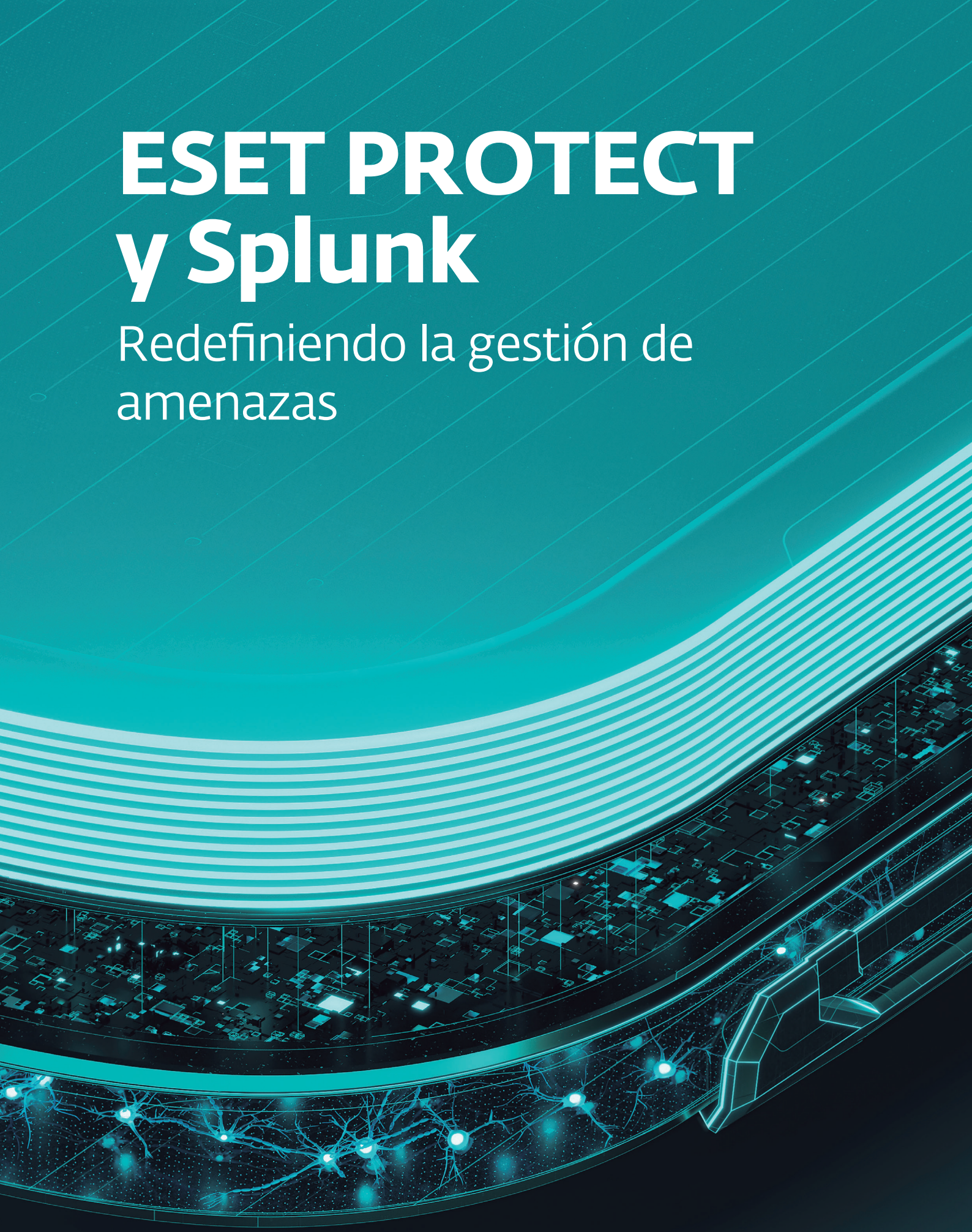
ESET PROTECT y Splunk

Redefiniendo la gestión de amenazas



Digital Security
Progress. Protected.

RESUMEN DE LA SOLUCIÓN

La protección de endpoint de vanguardia se une a la analítica avanzada

En el panorama actual de la ciberseguridad, las empresas se enfrentan a amenazas cada vez más complejas que requieren soluciones potentes e integradas. Los analistas de seguridad y los administradores de IT a menudo se ven abrumados por datos de seguridad fragmentados, lo que provoca una visibilidad incompleta y respuestas tardías. Estos desafíos son especialmente urgentes para los responsables de operaciones de seguridad (SOC Managers) y los CISOs/CIOs, quienes necesitan soluciones centralizadas y automatizadas para gestionar su seguridad de manera eficaz.

ESET PROTECT se integra perfectamente con **Splunk** para consolidar las alertas de seguridad y la telemetría en una sola interfaz. La integración permite a tu empresa investigar amenazas rápidamente, automatizar flujos de trabajo y gestionar la seguridad.

ESET PROTECT aprovecha su galardonada tecnología multicapa para detectar y neutralizar las ciberamenazas más sofisticadas. Cuando se combina con la sólida analítica de datos y conocimientos de seguridad de Splunk, esta integración ofrece una solución integral para mejorar la visibilidad, acelerar los tiempos de respuesta y simplificar la gestión de la seguridad.

Beneficios clave

DETECCIÓN AVANZADA DE AMENAZAS

Aprovecha el poder de la tecnología multicapa de ESET para identificar y mitigar ciberamenazas complejas.

RESPUESTA EN TIEMPO REAL

Benefíciate de alertas inmediatas y respuestas automatizadas ante posibles incidentes de seguridad, asegurando un rápido confinamiento y resolución.

GESTIÓN CENTRALIZADA

Disfruta de la comodidad de una sola consola para la monitorización y gestión de toda la seguridad.

ESCALABILIDAD

Adáptate a las crecientes necesidades de las empresas con soluciones flexibles diseñadas para escalar sin esfuerzo.

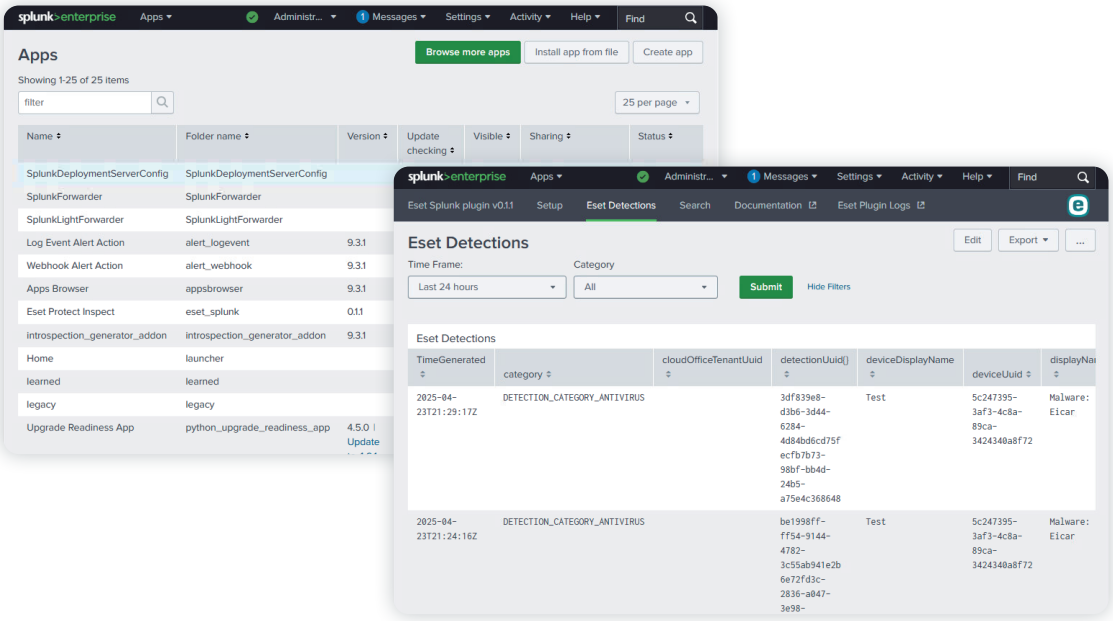
CONFORMIDAD

Cumple con la norma de conformidad mediante medidas integrales de protección de datos.

Cómo funciona

ESET PROTECT se integra con Splunk utilizando métodos basados en Syslog y API. La integración con Syslog permite que ESET PROTECT envíe registros a Splunk en tiempo real, mientras que la integración por API permite que Splunk consulte a ESET PROTECT para obtener registros de amenazas, eventos y detecciones. Esta integración garantiza que tu equipo de seguridad pueda agregar los eventos de detección de ESET con la telemetría de seguridad más amplia de Splunk, proporcionando una visión holística y reduciendo la carga manual.

- Integración basada en Syslog: Exporta sin problemas eventos en formato Syslog desde ESET PROTECT a Splunk para la transmisión y correlación de eventos en tiempo real.
- Integración basada en API: Utiliza las API REST de ESET para permitir que Splunk consulte y obtenga directamente eventos de seguridad y telemetría relevantes, mejorando la toma de decisiones basada en datos.



Gestión de amenazas de siguiente nivel en acción

ESCENARIO DE EJEMPLO

Los sensores de endpoint de ESET identifican una IP maliciosa como un servidor de comando y control (C2) que se comunica con múltiples endpoints.

FLUJO DE TRABAJO

1. DETECCIÓN: ESET PROTECT marca tráfico sospechoso desde un endpoint hacia una IP C2.

2. REENVÍO DE EVENTOS: ESET envía el evento de detección (a través de Syslog o API REST) a Splunk en tiempo real.

3. CORRELACIÓN: Splunk correlaciona automáticamente esta IP con otros registros de red, identificando múltiples endpoints que se comunican con la misma dirección maliciosa.

4. RESPUESTA AUTOMATIZADA: Una alerta automatizada de Splunk activa una llamada API REST de vuelta a la consola de ESET PROTECT o a la solución de firewall de gateway, indicándole que bloquee la IP maliciosa en toda la red.

5. CONFIRMACIÓN: El bloqueo se confirma y se informa en Splunk, proporcionando visibilidad de extremo a extremo para el equipo de seguridad.

Acerca de ESET

DEFENSA PROACTIVA.
MINIMIZA LOS RIESGOS CON LA PREVENCIÓN.
Experimenta la mejor protección de su clase gracias a la inteligencia sobre amenazas cibernéticas global de ESET, desarrollada internamente, recopilada y analizada durante más de 30 años, que impulsa nuestra extensa red de I+D liderada por investigadores reconocidos en la industria. ESET PROTECT, nuestra plataforma de ciberseguridad XDR cloud-first, combina prevención de nueva generación, detección y capacidades de búsqueda proactiva. ESET protege tu negocio para que puedas aprovechar todo el potencial de la tecnología.

Acerca de Splunk

Splunk es un proveedor líder de soluciones de analítica de datos y seguridad. La plataforma de Splunk permite a las empresas obtener información en tiempo real de sus datos, mejorando su capacidad para detectar, investigar y responder a amenazas de seguridad. Al integrarse con ESET, Splunk ofrece una poderosa combinación de protección de endpoint y analítica de seguridad integral.