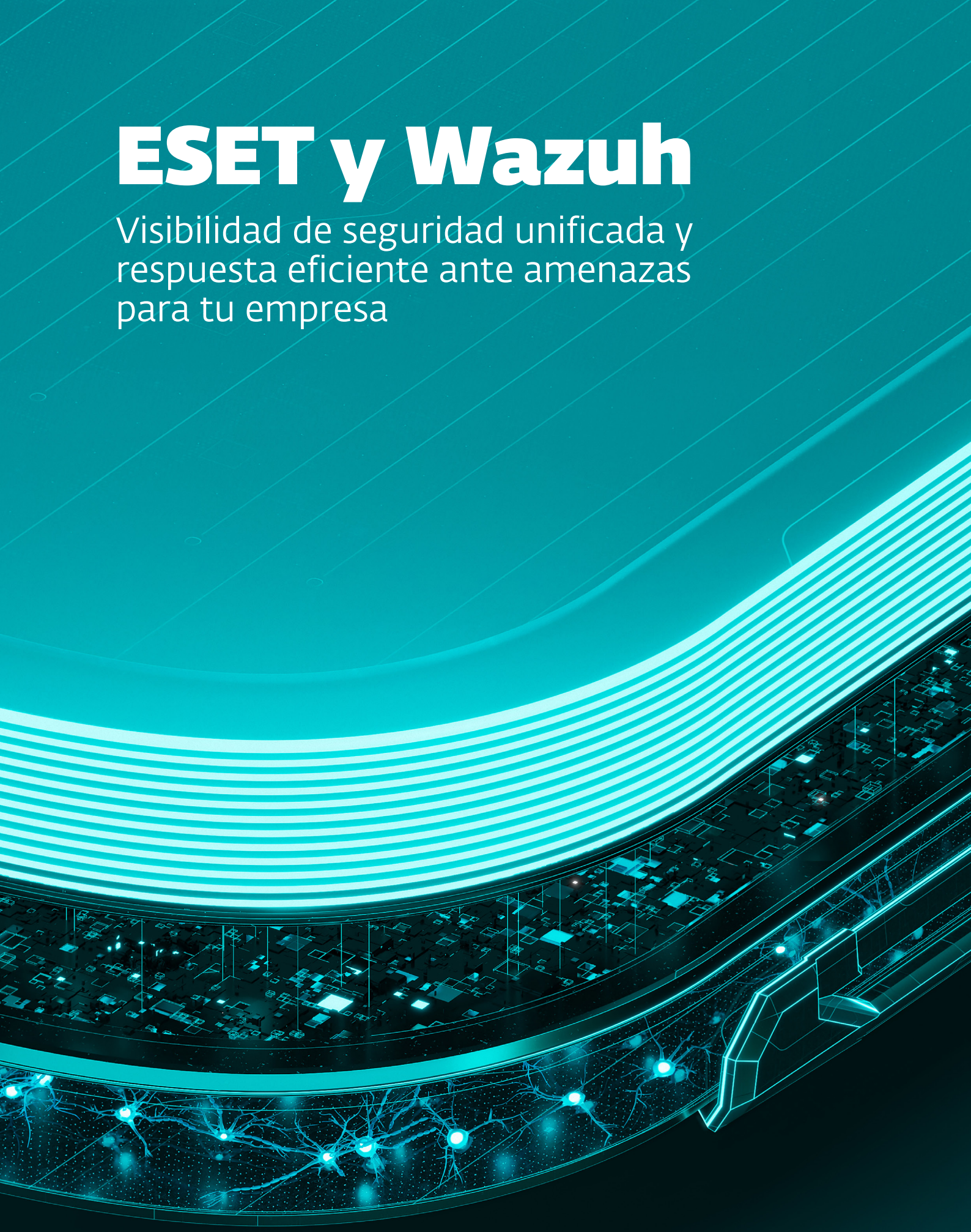
# ESET y Wazuh

## Visibilidad de seguridad unificada y respuesta eficiente ante amenazas para tu empresa



eset Digital Security
Progress. Protected.

RESUMEN DE LA SOLUCIÓN

# Mejora de la ciberseguridad con una integración perfecta

Los profesionales de la seguridad, como los analistas de seguridad y los administradores de IT, se enfrentan a retos cada vez mayores en materia de ciberseguridad y necesitan soluciones rentables para monitorizar y responder a las amenazas de forma eficaz. Tanto las pequeñas y medianas empresas (pymes) como las grandes empresas deben lidiar con grandes volúmenes de datos de seguridad, una visibilidad incompleta y recursos limitados en múltiples consolas de seguridad. Estos retos pueden provocar retrasos en la detección y respuesta a las amenazas, lo que aumenta el riesgo de brechas de seguridad y pérdida de datos.

La integración de ESET con Wazuh proporciona una plataforma de seguridad unificada que consolida las alertas de seguridad, la telemetría y los incidentes en un único panel. Esta integración mejora la capacidad de las empresas para detectar, investigar y responder a las amenazas de forma más eficaz. Al aprovechar la integración basada en API, Wazuh puede consultar y extraer eventos de seguridad, incidentes y telemetría relevantes directamente de:

### ESET PROTECT PLATFORM

La galardonada plataforma de protección de endpoints de ESET, que ofrece capacidades avanzadas de detección y prevención de amenazas.

### ESET INSPECT

El módulo de Detección y respuesta ampliada (XDR) de la plataforma que proporciona una visibilidad profunda de las actividades de los endpoints y capacidades avanzadas de búsqueda de amenazas.

### ESET CLOUD OFFICE SECURITY

El módulo de protección de correo electrónico y aplicaciones en la nube para empresas de ESET (MS365, Google Workspace), que protege el correo electrónico y las herramientas de colaboración basadas en la nube contra malware, phishing y otras amenazas.

Esta integración perfecta garantiza que los equipos de seguridad tengan una visión completa de su postura de seguridad, lo que les permite correlacionar los datos de los endpoints con la información de seguridad de la red y la nube. La plataforma unificada reduce la complejidad de la gestión de múltiples soluciones de seguridad, lo que permite a los profesionales de la seguridad centrarse en la gestión proactiva de amenazas y la respuesta a incidentes.

# VENTAJAS PRINCIPALES

## VISIBILIDAD DE SEGURIDAD UNIFICADA

Consolida los datos de seguridad de los endpoints, la red y la nube en una única consola para obtener una detección y respuesta integrales ante las amenazas.

## POSTURA DE SEGURIDAD MEJORADA

Al incorporar datos de alta calidad de ESET, las empresas optimizarán su postura de seguridad.

## CORRELACIÓN AUTOMATIZADA DE DATOS

Reduce los gastos generales manuales y los tiempos de respuesta con la ingesta y correlación automatizadas de datos.

## MAYOR EFICIENCIA

Los equipos de seguridad pueden hacer más con menos herramientas y menos intervención manual, lo que mejora la eficiencia general.

# CARACTERÍSTICAS PRINCIPALES

## TRANSMISIÓN DE ALERTAS EN TIEMPO REAL

Transmite las alertas de los endpoints de ESET directamente a Wazuh en tiempo real, lo que permite una correlación inmediata con los registros del firewall, los datos de IDS/IPS y las actividades de los usuarios.

## DATOS CATEGORIZADOS

Utiliza la funcionalidad de reglas de Wazuh para clasificar los registros de ESET en categorías existentes y organizar los datos de forma adecuada.

## ACCIONES AUTOMATIZADAS

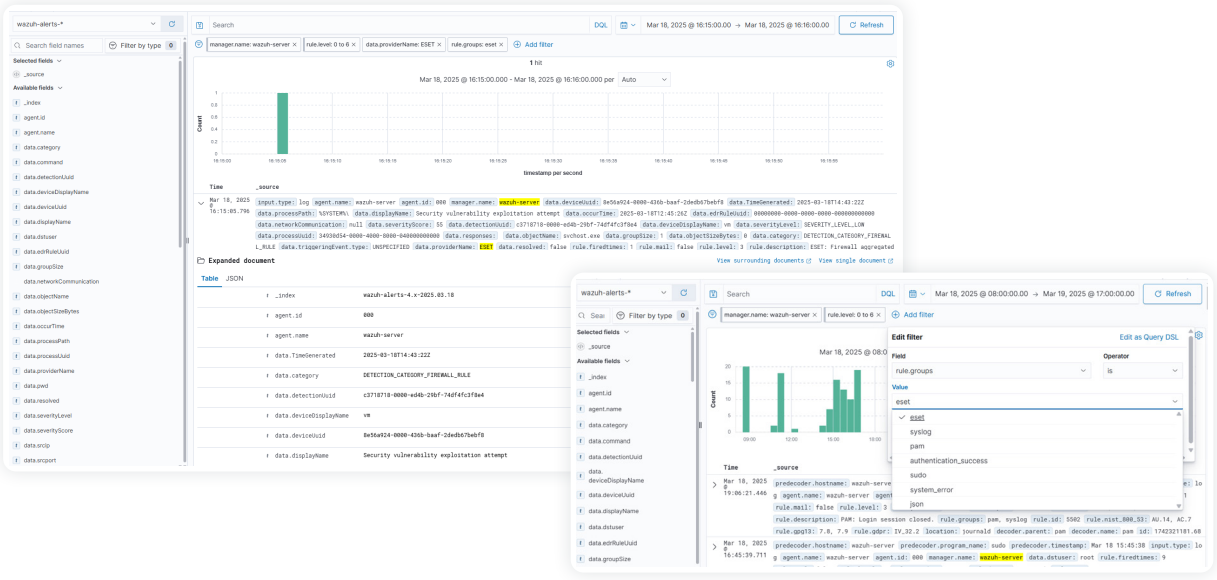
Las capacidades de alerta y flujo de trabajo de Wazuh pueden activar automáticamente acciones de contención y corrección en los endpoints a través de las API de gestión de ESET.

## PROTECCIÓN AVANZADA PARA EL CORREO ELECTRÓNICO Y LAS APLICACIONES PARA EMPRESA

Garantiza que el correo electrónico, el vector de amenazas número uno, recibe una protección proactiva de ESET que va más allá de la protección integrada de Microsoft365 y Google Workspace.

# CÓMO FUNCIONA

La integración funciona mediante el uso de API REST (HTTPS) para consultas seguras y recuperación de datos. Wazuh ejecuta una aplicación proporcionada que consulta ESET PROTECT, ESET Inspect y ESET Cloud Office Security para detectar amenazas en tiempo real. A continuación, los datos se ponen a disposición a través de PublicAPI para Wazuh, lo que permite una integración perfecta y una visibilidad de la seguridad unificada.



## Acerca de ESET

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

Disfruta de la mejor protección gracias a la inteligencia sobre ciberamenazas global de ESET, recopilada y examinada durante más de 30 años, que impulsa nuestra amplia red de I+D dirigida por investigadores de renombre en el sector. 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 Wazuh

Wazuh es una solución de monitorización de seguridad y cumplimiento normativo de código abierto que unifica las capacidades XDR y SIEM y ayuda a las empresas a detectar y responder a las amenazas de forma eficaz. Centrada en la rentabilidad y la escalabilidad, Wazuh presta servicio tanto a pymes como a grandes empresas, proporcionando monitorización de seguridad personalizable en infraestructuras complejas. Wazuh se integra con diversas plataformas para ofrecer una visibilidad y protección completas, lo que garantiza que los equipos de seguridad puedan gestionar y mitigar los riesgos de forma eficaz.

eset® Digital Security
Progress. Protected.

RESUMEN DE LA SOLUCIÓN