Cynet 360 AutoXDR™

La ciberseguridad integral nunca ha sido tan fácil

El enfoque actual para abordar la seguridad ha quedado obsoleto.

Actualmente, las organizaciones se ven obligadas a utilizar sistemas de seguridad por capas costosos, complejos y basados en múltiples productos, con laboriosos procesos manuales que agotan los recursos y las fuerzas de los equipos responsables de la seguridad informática. Peor aún, este enfoque inconexo y con un alto consumo de recursos les impide además tener una buena visibilidad y los expone a ataques sigilosos.

Devuelva el sentido común a su sistema de ciberseguridad con un nuevo enfoque que proteja a su organización de forma fácil y sin estrés.

Ciberseguridad simplificada.

La plataforma XDR de extremo a extremo de Cynet, automatizada de forma nativa, fue diseñada específicamente para equipos de ciberseguridad de dimensiones reducidas. De implementación instantánea, extremadamente fácil de usar, respaldado por un servicio MDR gratuito 24/7 y proporcionado con el TCO más eficaz, el sistema Cynet permite a cualquier organización lograr una protección integral y eficiente, independientemente de sus recursos, del tamaño de su equipo de TI o de su capacidad técnica.

Con una visibilidad completa de los puntos de conexión, usuarios, redes, aplicaciones SaaS y en la nube, junto con una gran capacidad de respuesta automatizada, la visión de Cynet es lograr que los equipos de seguridad puedan poner su ciberseguridad en piloto automático y dediquen sus valiosos recursos a la gestión de la seguridad en vez de centrarse en atender las incidencias.

Beneficios clave

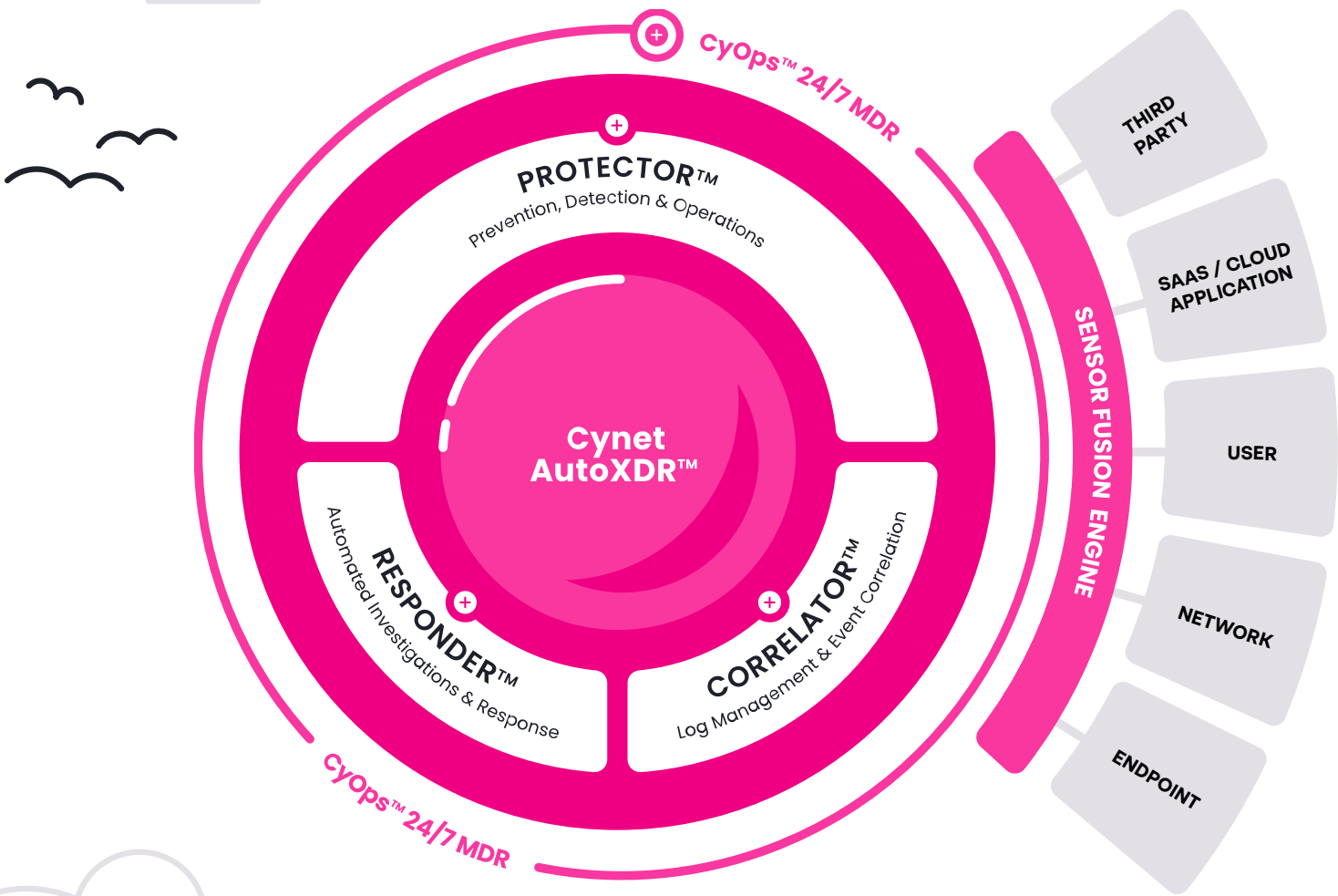
Obtenga protección de extremo a extremo
con una plataforma unificada de forma nativa para la detección, prevención, correlación, investigación y respuesta en todos los puntos de conexión, usuarios, redes, aplicaciones SaaS y en la nube.

Aproveche la automatización nativa de respuestas
para reducir al mínimo las tareas manuales y poder dedicar su tiempo a gestionar la seguridad en vez de centrarse en atender las incidencias.

Logre una visibilidad completa
para una protección precisa y exhaustiva contra las amenazas en todo su entorno.

Maximice el rendimiento de la inversión
con el coste total de propiedad (TCO) más eficaz y reduciendo los recursos requeridos.

Esté tranquilo las 24 horas del día, los 7 días de la semana
mientras el equipo proactivo de detección y respuesta gestionadas (MDR) de Cynet monitorea continuamente su entorno, brindando asistencia y orientación especializadas.



Visita www.cynet.com

Detenga las intrusiones y salga más temprano del trabajo

Con la plataforma de ciberseguridad unificada creada para equipos de seguridad de TI optimizados

Protector™

Prevención, detección, operaciones de TI y de seguridad

Previene y detecta amenazas utilizando las capacidades combinadas de NGAV, EDR, NDR, UBA, y tecnología de engaño, entre otros.

PROTECCIÓN DE PUNTOS DE CONEXIÓN: Protección inigualable contra amenazas avanzadas en puntos de conexión, incluyendo NGAV, control de dispositivos y protección de recursos críticos, entre otros.

DETECCIÓN EXTENDIDA DE AMENAZAS: La visibilidad ampliada en todos los puntos de conexión, redes y usuarios proporciona funcionalidades de protección en capas de EDR, tecnología de engaño, normas de análisis del comportamiento del usuario, normas de detección de red, entorno de pruebas e inteligencia de detección de amenazas lista para usar.

GESTIÓN DE LA POSTURA DE SEGURIDAD EN LA NUBE (CSPM) Y GESTIÓN DE LA POSTURA DE SEGURIDAD DEL SAAS (SSPM): Supervise y corrija los errores de configuración de aplicaciones SaaS y de la nube para eliminar los riesgos de seguridad.

OPERACIONES DE TI Y SEGURIDAD: Amplias funciones operativas incluidas de forma nativa, como higiene de TI, gestión de vulnerabilidades y capacidades de inventario de activos.

Responder™

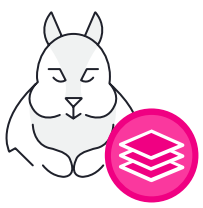
Investigación y respuesta automatizadas

Automatiza todas las acciones de investigación y respuesta requeridas en todo el entorno.

INVESTIGACIÓN AUTOMATIZADA: Cuando detecta una amenaza de alto riesgo, Cynet inicia automáticamente una investigación para descubrir instantáneamente la causa de fondo y el alcance real del ataque.

RESOLUCIÓN AUTOMATIZADA: Cynet proporciona la más amplia gama de acciones de resolución automatizadas para contener y remediar instantáneamente las amenazas detectadas en puntos de conexión, redes, usuarios y aplicaciones SaaS.

PROTOCOLOS DE RESOLUCIÓN: Siga las instrucciones de los protocolos de actuación incorporados o personalizados que combinan múltiples acciones de resolución para erradicar todos los rastros de amenazas identificadas.



Correlator™

Gestión de registros y correlación de eventos

Recopila y correlaciona datos de alerta y actividad en incidentes procesables, proporcionando capacidades esenciales de gestión de eventos e información de seguridad (SIEM).

ADMINISTRACIÓN CENTRALIZADA DE REGISTROS: Recopila e integra los datos de registro críticos necesarios para el análisis de amenazas utilizando un potente lenguaje de consulta junto con gráficos y paneles intuitivos.

CORRELACIÓN DE EVENTOS: Analiza las señales de los controles nativos de Cynet, los registros del sistema y cualquier otra fuente para correlacionar los datos en incidentes procesables.

CAPACIDADES FORENSES: Investigue amenazas y realice caza de amenazas con acceso instantáneo a artefactos forenses recopilados de agentes de Cynet, registros y otros recursos del sistema, utilizando potentes herramientas de búsqueda y visualización.

CyOps™ 24/7 MDR

Monitorización y respuesta continuos

Un equipo de detección y respuesta gestionadas de primer nivel que garantiza su seguridad y protección.

MONITORIZACIÓN 24/7: Garantiza la identificación y la gestión adecuada de las amenazas peligrosas las 24 horas del día. Ideal para equipos con recursos limitados.

RESPUESTA A INCIDENTES: Asistencia en respuesta remota a incidentes, con investigación, plan integral de resolución y orientación.

CAZA DE AMENAZAS: Búsqueda proactiva de amenazas ocultas en el entorno.

INFORMES SOBRE ATAQUES: Descripción general elaborada por escrito e información detallada sobre los aspectos técnicos del ataque.