Cortex XDR

Proteja todos los endpoints y reduzca los riesgos con un enfoque impulsado por la inteligencia artificial

Los ciberataques se producen ahora tres veces más rápido que hace sólo cuatro años. En el 20 % de los casos, el tiempo que transcurre desde el ataque inicial hasta la filtración de los datos es inferior a una hora.[1] Muchas de las herramientas de seguridad para endpoints no son proactivas y permiten la entrada de demasiadas amenazas. Además, abruman a los analistas con alertas poco contextualizadas y generan una sobrecarga operativa que aumenta tanto los costes como la complejidad.

1. *Informe 2025 de Unit 42 sobre la respuesta global a incidentes*, Palo Alto Networks Unit 42, febrero de 2025.

Para tener éxito en la defensa contra los ciberataques actuales, los equipos de operaciones de seguridad necesitan:

- **Seguridad centrada en la prevención** que detiene las amenazas antes de que accedan, para reducir el riesgo de infracción.
- **Contexto enriquecido e IA avanzada** para una detección, investigación y corrección de alta precisión.
- **Una única plataforma** para centralizar las operaciones y reducir el coste total de propiedad (TCO).

Cortex XDR® ofrece la seguridad de endpoints basada en IA más eficaz del mundo, probada por seis años de resultados excepcionales de MITRE ATT&CK®.[2] Su diseño exclusivo cierra estas brechas de seguridad, reforzando su postura a la vez que simplifica las operaciones. Cortex XDR le permite:

- **Prevenir con confianza:** Detenga los exploits avanzados, el malware y los ataques sin archivos en tiempo real con un agente unificado y fácil de implementar para endpoints y tiempo de ejecución en la nube.
- **Detectar ataques evasivos:** Vaya más allá del endpoint, aplicando la IA líder del sector a los datos de endpoint, red, nube, identidad y correo electrónico para descubrir lo que otras soluciones pasan por alto.
- **Eliminar el 98 % del ruido de alertas:** Reduzca drásticamente la carga de trabajo de los analistas agrupando automáticamente miles de problemas en unos pocos casos priorizados que muestran la historia completa del ataque.
- **Responder casi en tiempo real:** Detenga los ataques con la mejor automatización de su clase, agentes de IA, acciones rápidas dirigidas por analistas o nuestro servicio integrado ininterrumpido de Detección y respuesta gestionadas (MDR).

Un líder de mercado en el que puede confiar

Nuestro liderazgo en el mercado está validado por las evaluaciones más rigurosas del sector y valorado por miles de clientes en todo el mundo.

- **Rendimiento histórico de MITRE:** Palo Alto Networks es el primer proveedor que consigue un 100 % de detección a nivel técnico con Cortex XDR en las evaluaciones ATT&CK de MITRE, sin realizar cambios en la configuración, lo que refleja el rendimiento en el mundo real.[3]
- **Líder reconocido en 3 ocasiones:** Palo Alto Networks con Cortex XDR ha sido nombrado líder en el Magic Quadrant™ de Gartner® para plataformas de protección del endpoint por tercer año consecutivo.[4]
- **Máxima disposición a recomendar:** Cortex XDR fue clasificada por los profesionales de la seguridad como la solución para endpoints más recomendada de todos los proveedores de Gartner® Customers' Choice™ para plataformas de protección de endpoints.[5]

Cómo detiene Cortex XDR los ataques sofisticados

Cortex XDR ofrece lo que los equipos de seguridad necesitan de una solución moderna de defensa de endpoints, al tiempo que proporciona la plataforma fundamental para una transformación del SOC impulsada por la IA.

1. Reduce el riesgo con una prevención líder del sector

Nuestros expertos en investigación de Unit 42® aprovechan la capacidad masiva de Palo Alto Networks — incluidos nuestros más de 70.000 clientes de todos los sectores en todo el mundo— para descubrir los últimos comportamientos de amenazas y entrenar la IA dentro del agente Cortex XDR. Este agente único y ligero bloquea amenazas sofisticadas en tiempo real con funciones rigurosamente probadas que funcionan nada más sacarlo de la caja. Utiliza varios métodos para bloquear las amenazas:

- **Protección frente a amenazas basadas en el comportamiento:** Detiene las amenazas sin archivos y los nuevos patrones de ataque supervisando los procesos en busca de combinaciones de actividades que indiquen un comportamiento malicioso.
- **Protección antimalware de día cero:** Examina más de 20.000 características de archivos y utiliza el aprendizaje automático (ML) para detener al instante el malware desconocido.
- **Prevención de exploits:** Supervisa cientos de procesos de endpoints para bloquear las técnicas utilizadas para explotar aplicaciones, independientemente de si la vulnerabilidad se ha visto antes.

2. "MITRE ATT&CK Enterprise Evaluations Brings the Heat in Round 6", Palo Alto Networks, diciembre de 2024.
3. Palo Alto Networks, "Evaluaciones de MITRE ATT&CK Enterprise".
4. "A Leader in the 2025 Gartner Magic Quadrant for EPP - 3 Years Running", Palo Alto Networks, 17 de julio de 2025.
5. "Cortex XDR Named 2025 Gartner Customers' Choice for Endpoint Security", Palo Alto Networks, 28 de mayo de 2025.

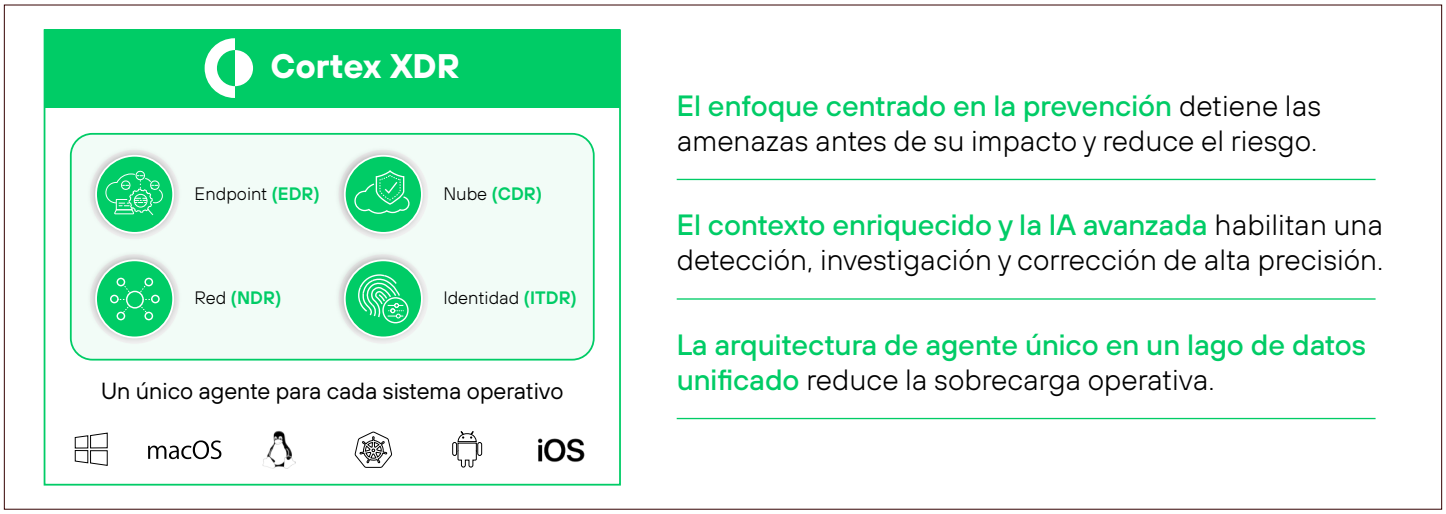

Figura 1. Descripción general de la solución Cortex XDR

2. Ahorra tiempo a los analistas gracias a una precisión de detección inigualable

El agente Cortex XDR recopila una amplia gama de telemetría del endpoint y de fuentes ampliadas, creando un contexto rico que permite a los análisis de seguridad más precisos del sector detectar amenazas a la velocidad de la máquina. Cortex XDR marcó un nuevo hito en el sector al ser la primera solución para endpoints que obtuvo una puntuación del 100 % en detección técnica en la sexta ronda de evaluaciones de MITRE.[6]

Al utilizar esta base de datos ricos en contexto, Cortex XDR agrupa automáticamente las detecciones relacionadas en casos únicos y priorizados que cuentan la historia completa del ataque. Este enfoque agiliza la investigación y reduce la selección de alertas en hasta un 98 %[7], lo que supone un ahorro diario en horas de trabajo para sus analistas.

Automatización fiable con transparencia

La automatización en Cortex XDR viene con total transparencia para su equipo, proporcionando explicaciones claras y comprensibles para la lógica de detección y las acciones automatizadas. Por ejemplo, cuando Cortex XDR genera un problema y crea un caso, explica la lógica de aprendizaje automático que subyace a su puntuación de riesgo, lo que permite a su equipo confiar en el sistema y actuar con decisión.

3. Acelera la respuesta con rapidez y precisión

Con el contexto completo de un ataque, su equipo puede responder con rapidez y precisión. Aproveche los más de 100 libros de estrategias integrados en Cortex XSOAR® para la corrección automatizada y utilice el asistente Cortex AgentiX Assistant para dirigir una flota de agentes de IA que investigan y actúan a la velocidad de la máquina. Para acciones quirúrgicas dirigidas por analistas, Live Terminal proporciona acceso directo mediante Secure Shell (SSH) a los hosts comprometidos para contener las amenazas de forma instantánea.

4. Reduce el coste total de propiedad con la base del SOC impulsado por IA

Cortex XDR reduce la sobrecarga operativa y el coste total de propiedad al proteger los principales sistemas operativos (Windows, macOS y Linux) y tiempos de ejecución en la nube (por ejemplo, Kubernetes) con una arquitectura de agente único. Además de consolidar la seguridad de los endpoints, es el primer paso en el camino hacia la transformación del SOC. Con un único agente implementado y sus datos de seguridad centralizados en Cortex Extended Data Lake™ (XDL), dispondrá de un camino sin fricciones hacia Cortex XSIAM®, la plataforma impulsada por IA que unifica y transforma todo su SOC.

6. Palo Alto Networks, "Evaluaciones de MITRE ATT&CK Enterprise".
7. North Dakota IT protege a la ciudadanía con operaciones de seguridad integradas e impulsadas por IA, Palo Alto Networks, November 18, 2024.

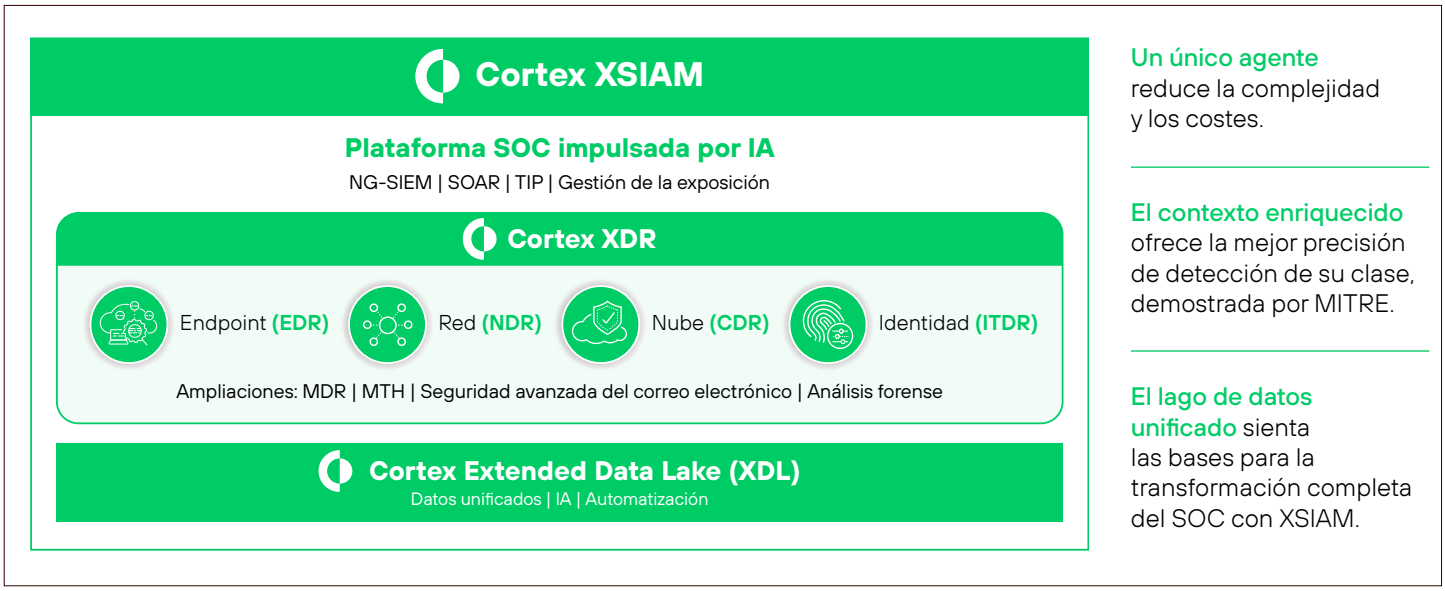

Figura 2. Arquitectura de agente único en un lago de datos unificado

Seguridad y control total del endpoint

Cortex XDR proporciona todas las herramientas esenciales necesarias para reforzar y controlar sus endpoints desde una única consola, utilizando el mismo agente unificado.

- **Control de dispositivos:** Mitigue los riesgos de los soportes físicos supervisando y gestionando el acceso a dispositivos USB y Bluetooth con políticas granulares.
- **Cortafuegos del host y cifrado de disco:** Gestione de forma centralizada los cortafuegos basados en hosts para Windows y macOS, e imponga el cifrado de disco completo (BitLocker o FileVault) para cumplir las normativas.
- **Seguridad móvil:** Amplíe la protección frente a amenazas de nivel empresarial y el control del tráfico a sus dispositivos corporativos iOS y Android.

Complementos de seguridad

Amplíe las capacidades de Cortex XDR con potentes módulos integrados:

- **Seguridad en tiempo de ejecución en la nube:** Evite los ataques a la nube en tiempo real con la mejor protección de su clase proporcionada por el agente Cortex XDR para máquinas virtuales, contenedores, Kubernetes y cargas de trabajo sin servidor.
- **Detección y respuesta a amenazas de identidad (ITDR):** Descubra las amenazas basadas en la identidad analizando el comportamiento de usuarios y entidades, identificando las cuentas comprometidas y permitiendo una respuesta rápida a las amenazas internas.
- **Advanced email security:** Detenga los ataques por correo electrónico en tiempo real con un motor de análisis basado en inteligencia artificial que evalúa la intención de cada mensaje. Con el contexto de los datos de endpoints, identidades y redes, los analistas pueden comprender cómo se inicia un ataque, se propaga y repercute en la organización.
- **Información del host:** Gestione de forma proactiva su superficie de ataque con una evaluación completa de vulnerabilidades y un inventario de hosts.
- **Análisis forense:** Acelere las inmersiones profundas con datos forenses enriquecidos, incluida la memoria volátil, para determinar el origen y el alcance de un ataque.

Gestión e implementación flexibles

Implemente rápidamente y aumente su equipo con servicios 24 horas al día, 7 días a la semana, dirigidos por expertos.

- **Arquitectura para la nube:** Cortex XDR elimina la necesidad de almacenamiento local de logs. El agente ligero se instala y actualiza sin necesidad de reiniciar el sistema.
- **Servicios gestionados por expertos:** Para mayor tranquilidad, amplíe su equipo con nuestra Detección y respuesta gestionadas de Unit 42. Obtendrá supervisión, investigación y respuesta las 24 horas del día, los 7 días de la semana, para acabar con los ataques con el mejor tiempo medio de respuesta (MTTR) de su clase.

En resumen: Operaciones de seguridad más maduras

Cortex XDR se traduce directamente en valor empresarial para que su SOC se beneficie de:

- **Reducción del trabajo manual:** Sus equipos dedican mucho menos tiempo a la correlación, el triaje de alertas y la investigación inicial.
- **Respuestas más rápidas y precisas:** Los equipos pueden centrarse en las amenazas validadas y priorizadas, y aprovechar la corrección automatizada.
- **Analistas con mayores capacidades:** Su organización puede liberar personal cualificado para tareas estratégicas como la caza de amenazas y la automatización más avanzada.

Tabla 1. Opciones de licencia de Cortex XDR

Característica	XDR Prevent	XDR Pro por endpoint
Prevención de amenazas en el endpoint Evite el malware, el ransomware, los exploits y los ataques sin archivos.	✓	✓
Controles de los endpoints Proteja los endpoints con control de dispositivos, cortafuegos y cifrado de discos.	✓	✓
Detección de amenazas a endpoints Descubra ataques en tiempo real con miles de detectores analíticos integrados basados en ML.	—	✓
Casos unificados con puntuación de riesgo Cada detección relacionada se agrupa en un único caso y se puntúa según el riesgo.	—	✓
Respuesta automatizada y dirigida por analistas Más de 100 guías integradas y acciones rápidas integradas permiten una rápida corrección.	—	✓
Análisis de detección extendidos y acciones de respuesta (red, nube, identidad)	—	Complemento
Seguridad en tiempo de ejecución en la nube	—	Complemento
Detección y respuesta a amenazas de identidad (ITDR)	—	Complemento
Advanced Email Security	—	Complemento
Búsqueda de amenazas gestionada	—	Complemento
Detección y respuesta gestionadas	—	Complemento
Datos ampliados sobre la caza de amenazas	—	Complemento
Información del host	—	Complemento
Investigación forense	—	Complemento

paloalto NETWORKS

Oval Tower
De Entrée 99 - 197

Tel.: +31 20 888 1883
Ventas: +1.866.320.4788
Asistencia técnica: +1.866.898.9087

www.paloaltonetworks.es

cortex_ds_cortex-xdr_121025