# Cómo sobrevivir al ransomware: todo lo que hay que saber

En los últimos tiempos, los medios de comunicación se han hecho eco de los incesantes ataques de ransomware que afectan a distintos sectores. Desde Trojan.Gpcoder, el primer ransomware moderno que utiliza un archivo adjunto de correo electrónico infectado, hasta los sonados ataques contra Colonial Pipeline (uno de los principales operadores de oleoductos de Estados Unidos) y JBS Foods (la mayor empresa cárnica del mundo), cada vez está más claro que los profesionales de la seguridad se enfrentan a enemigos de gran envergadura.

El primer ataque de ransomware se detectó allá por 2005, básicamente porque los sistemas de pago en línea todavía no se habían generalizado antes de esa fecha. A medida que se fueron perfeccionando las metodologías de ataque a través de las telecomunicaciones, empezaron a aparecer las primeras víctimas, que recibían mensajes SMS con peticiones de rescate. En 2008 entró en escena el bitcoin (aunque la fecha oficial de lanzamiento fue enero de 2009), capaz de anonimizar las transacciones en gran medida y, por tanto, de hacerlas difíciles de rastrear.

**Tabla 1: Ransomware: antes y ahora**

| | Infiltración | Actividad posterior al exploit | Entidades afectadas | Rescates |
|---|---|---|---|---|
| **Antes** | • Protocolo de escritorio remoto (RDP)<br>• Correos electrónicos de *phishing* | • Tiempos de permanencia breves<br>• Reconocimiento básico y escalada de privilegios | • Particulares<br>• Organizaciones pequeñas con hasta 100 endpoints<br>• Muchas organizaciones sanitarias<br>• Pequeños equipos | • Importes reducidos, normalmente inferiores a un par de bitcoins (1 bitcoin = 13 620 USD) |
| **Ahora** | RDP y *phishing*<br>Puntos de entrada de CVE:<br>• Vulnerabilidades recientes del equilibrador de carga<br>• Vulnerabilidades generales de la infraestructura web | Todavía se ven algunos TTP antiguos, pero también:<br>• Sistema basado en PowerShell<br>• RAT<br>• BloodHound<br>• Dridex, Emotet, Trickbot<br>• Eliminación de copias de seguridad | • Empresas de todos los tamaños<br>• Ninguna empresa u organización es inmune | • Cientos de miles o incluso millones de dólares<br>• El pago medio por ransomware subió un 82 % desde 2020 hasta alcanzar la cifra récord de 570 000 USD en la primera mitad de 2021[1]<br>• Las cuantías se suelen fijar en función del valor que los ciberdelincuentes otorguen al negocio |

## Introducción al ransomware: aspectos básicos

El ransomware es un modelo de negocio delictivo que utiliza software malicioso para cifrar y bloquear los datos de un sistema y exigir el pago de un rescate a cambio de desbloquear el acceso. Aunque se trata de un problema cada vez más acuciante, el ransomware se puede prevenir —o, al menos, minimizar los daños que provoca— mediante una formación adecuada, unos ajustes específicos en el entorno informático y la implementación de tecnología de seguridad avanzada en los endpoints, como por ejemplo soluciones de detección y respuesta ampliadas (XDR, por sus siglas en inglés).

Existen dos tipos básicos de ransomware. El *ransomware de cifrado*, que es el más común, cifra archivos y datos, mientras que en el *ransomware de bloqueo* bloquea equipos u otros dispositivos, de modo que las víctimas no pueden utilizarlos.

El ransomware de bloqueo únicamente bloquea el dispositivo; los datos que contiene suelen mantenerse intactos. En cuanto se elimina el malware, se puede acceder a los datos con normalidad. Incluso si el malware no se puede eliminar fácilmente, con frecuencia los datos se pueden recuperar instalando la unidad de almacenamiento (normalmente un disco duro) a otro ordenador que funcione.

En el caso del ransomware de cifrado, los datos se cifran, por lo que, aunque se elimine el malware del dispositivo o se traslade la unidad de almacenamiento a otro equipo, sigue siendo imposible acceder a ellos. Normalmente, el ransomware de cifrado no ataca a los archivos críticos del sistema, lo que permite que el dispositivo siga funcionando a pesar de estar infectado; al fin y al cabo, es posible que se necesite el dispositivo para pagar el rescate.[2]

En la mayoría de los ataques de ransomware se siguen estos pasos, a menos que se mitigue el ataque o que la víctima se niegue a pagar el rescate:

1. **Se ataca el sistema y se toma el control.** La mayoría de los ataques comienzan con el método de *spear phishing*: el usuario recibe un correo electrónico fraudulento con un archivo adjunto infectado y lo abre, lo que pone en riesgo el sistema. Esto puede afectar a un solo host, como un ordenador o un dispositivo móvil. A continuación, el host afectado establece comunicaciones con un servidor de comando y control. En ese momento, el atacante podría moverse lateralmente desde el host inicial hacia otros sistemas de la organización para maximizar el alcance del ataque de ransomware.
2. **Se impide el acceso al sistema.** Una vez infectado el sistema, el atacante identifica y cifra determinados tipos de archivos que pueden ser valiosos para la víctima, como los documentos de trabajo (.doc, .xls, .pdf, etc.) o bien impide por completo el acceso al sistema mediante pantallas de bloqueo o tácticas de intimidación.

1. Tao Yan et al., *Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228)* (disponible en inglés), Unit 42, 28 de diciembre de 2021, https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/.
2. Ronny Richardson y Max M. North, *Ransomware: Evolution, Mitigation and Prevention* (disponible en inglés), Kennesaw State University, 1 de enero de 2017, https://digitalcommons.kennesaw.edu/facpubs/4276.

3. **Se comunican al propietario del dispositivo el ataque, el importe del rescate y los pasos que debe seguir.** El atacante notifica el ataque de ransomware a las víctimas, a menudo mediante una nota de rescate con las instrucciones de pago y los pasos que debe seguir para desbloquear los dispositivos.
4. **Se acepta el pago del rescate.** El atacante debe tener una forma de recibir los pagos de los rescates al margen de la ley. Por este motivo, se suelen utilizar criptomonedas anónimas como el bitcoin para realizar estas transacciones.
5. **Se promete la restitución del acceso tras la recepción del pago.** Si no se restablece el acceso a los sistemas afectados, este método de ataque deja de ser efectivo, puesto que nadie pagará un rescate si no tiene la garantía de que se le restituirán sus objetos de valor.

## Métodos de ataque comunes

Para prevenir mejor el ransomware, es fundamental comprender las tácticas que utilizan los atacantes. Se utilizan diferentes variantes de ransomware a través de varios vectores de ataque; por ejemplo, a través de la red o las aplicaciones SaaS o atacando el endpoint directamente. Esta información le permitirá centrar sus controles de seguridad en los ámbitos más susceptibles de ser atacados y, en consecuencia, reducir el riesgo de infección.

### Archivos adjuntos de correo electrónico maliciosos

En el pasado, los atacantes enviaban correos electrónicos como si procedieran de una fuente fiable, como el departamento de recursos humanos o de informática, y adjuntaban un archivo malicioso, como un archivo portable ejecutable (PE), un documento de Word o un archivo .JS. El destinatario abría el archivo adjunto pensando que el correo electrónico procedía de una fuente de confianza. Una vez abierto el archivo, la carga útil de ransomware se descargaba sin que el usuario lo advirtiese, el sistema se infectaba y se pedía un rescate para desbloquear los archivos. Hoy en día, las infecciones de malware dan acceso a los atacantes, que posteriormente implementan el ransomware.

### Enlaces de correo electrónico maliciosos

De forma similar a los archivos adjuntos maliciosos, este tipo de enlaces son direcciones URL que se incluyen en el cuerpo del correo electrónico. Estos correos electrónicos también se reciben de un emisor u organización que se considera de confianza. Al hacer clic en el enlace, desde la dirección URL se descargan archivos maliciosos a través de la web, el sistema se infecta y se pide un rescate para desbloquear los archivos.

### Credenciales vulnerables

Los atacantes de ransomware también pueden comprar credenciales a los agentes de acceso inicial (IAB, por sus siglas en inglés) para ahorrarse el proceso inicial de ataque a la víctima. Los IAB son individuos que recopilan credenciales y las venden al mejor postor. Aunque no solo son útiles a los atacantes de ransomware, estos se benefician claramente del sistema, normalmente al principio de la intrusión, ya que les permite realizar un reconocimiento para identificar redes con aplicaciones o dispositivos vulnerables, como redes VPN, protocolos de escritorio remoto (RDP, por sus siglas en inglés) abiertos o servidores con vulnerabilidades de software expuestas. Este vector se puede evitar aplicando prácticas recomendadas de reconocida eficacia, como la autenticación de dos factores y otros mecanismos de identificación.

## ¿Quién está en riesgo?

Se podría pensar que solo las grandes empresas son objetivo del ransomware, pero lo cierto es que las pymes no son inmunes a los ataques; es más, representan más de la mitad del total de víctimas, según una audiencia del Comité Judicial del Senado de EE. UU. («America Under Cyber Siege: Preventing and Responding to Ransomware Attacks») celebrada en julio de 2021.

Los ataques de ransomware pueden tener una gran repercusión pública, ya que las organizaciones víctimas pueden sufrir graves daños o verse obligadas a cerrar directamente, como demuestran los recientes ataques a hospitales de todo Estados Unidos. La información de identificación personal (PII, por sus siglas en inglés) puede ser una verdadera mina de oro para los ciberdelincuentes, que pueden venderla o subastarla en la dark web.

Los atacantes se han dado cuenta de que se trata de un negocio lucrativo con pocas barreras de entrada. Un ejemplo claro es el modelo de ransomware como servicio, en el que los afiliados utilizan herramientas de ransomware ya desarrolladas para ejecutar ataques de este tipo. En consecuencia, el ransomware está desplazando a otros modelos de negocio de la ciberdelincuencia. Además, los atacantes son cada vez más sofisticados a la hora de determinar el valor de la información en riesgo, evaluar la disposición a pagar de la organización víctima del ataque y exigir rescates más altos.

> **«El ransomware no solo afecta a los bolsillos de las grandes empresas como Colonial Pipeline y JBS. Las pequeñas empresas ya operan con márgenes estrechos, y muchas están al borde del abismo por la pandemia».**
>
> Chuck Grassley, Miembro de la Minoría del Comité Judicial del Senado de EE. UU.

## Más plataformas vulnerables

Aunque, en el pasado, los atacantes se centraban casi exclusivamente en los sistemas Microsoft Windows®, la aparición de ransomware para Android®, macOS® X y ahora también Linux demuestra que ningún sistema operativo es inmune a estos ataques. Casi todos los ordenadores o dispositivos con conexión a Internet son víctimas potenciales del ransomware, lo que sin duda es preocupante, teniendo en cuenta la proliferación de dispositivos IdC y, más recientemente, la ampliación de la superficie de ataque debido al auge del teletrabajo.

## Las cadenas de suministro, en el punto de mira

En 2021, Kaseya VSA, una multinacional de software de gestión de TI, se convirtió involuntariamente en la viva imagen de los ataques a la cadena de suministro cuando sufrió una brecha provocada por una variante especialmente virulenta del ransomware Sodinokibi. Conocido como «REvil», es un ransomware como servicio (RaaS, por sus siglas en inglés) que distribuye infecciones de malware mediante los afiliados, a quienes ofrece un porcentaje de los rescates pagados después de que los desarrolladores del ransomware reciban su parte.

Aprovechando una vulnerabilidad de software, los atacantes lograron acceder al software de Kaseya e instalaron el ransomware en la infraestructura de los clientes. El ataque tenía como objetivo exigir un rescate por los datos y recursos financieros de los clientes de Kaseya.

Al tratarse de una lacra mundial, organizaciones como la Agencia de la Unión Europea para la Ciberseguridad (ENISA) investigan e informan sobre la evaluación y estudio de los ataques a la cadena de suministro, entre otros. En su reciente informe *ENISA Threat Landscape for Supply Chain Attacks, 2021* (disponible en inglés),[3] destacan conclusiones como estas:

- Alrededor del 50 % de los ataques se atribuyeron a grupos de amenazas persistentes avanzadas (APT, por sus siglas en inglés) que los profesionales de la seguridad conocían bien.
- Alrededor del 42 % de los ataques analizados aún no se han atribuido a un grupo concreto.
- Alrededor del 62 % de los ataques a clientes se aprovecharon de su confianza en el proveedor.
- En el 62 % de los casos, emplearon la técnica del malware.
- Si nos fijamos en los activos afectados, en el 66 % de los incidentes, los atacantes se centraron en el código de los proveedores para afectar aún más a los clientes objetivo de los ataques.
- Alrededor del 58 % de los ataques a la cadena de suministro tenían como objetivo acceder a los datos (sobre todo datos de clientes, incluidos los datos personales y la propiedad intelectual) y alrededor del 16 %, a las personas.

Los ataques a la cadena de suministro son atribuibles al auge de las prácticas ágiles y de DevOps, que pueden acelerar los ciclos de desarrollo debido a unos plazos de lanzamiento de nuevas funciones y características normalmente agresivos, y a la consiguiente dependencia del código de terceros en las aplicaciones de los proveedores.

## El auge de la doble, triple e incluso *cuádruple* extorsión

En el caso de la doble extorsión, además de cifrar los datos, los atacantes de ransomware los roban para poner a la víctima aún más contra las cuerdas y obligarla a pagar el rescate exigido. Si esta decide no pagarlo, los atacantes los filtran en un sitio web creado a tal efecto (por lo general, alojado en la dark web) o en un dominio de la propia dark web creado y gestionado por ellos mismos. En estos momentos, hay al menos 16 variantes de ransomware distintas que amenazan con exponer información o utilizar sitios web de filtración de datos, y se prevé que otras vayan sumándose a la lista.[4]

En octubre de 2020, se denunció el primer caso de triple extorsión cuando se vulneraron los sistemas internos de Vastaamo, una clínica de psicoterapia finlandesa con 400 empleados y unos 40 000 pacientes. Después de intentar extorsionarlos con un rescate de 40 bitcoins (403 000 libras esterlinas; más de 500 000 dólares), los atacantes comenzaron a exigir los rescates a víctimas particulares, incluidos menores.

3. *ENISA Threat Landscape for Supply Chain Attacks* (disponible en inglés), Agencia de la Unión Europea para la Ciberseguridad, 29 de julio de 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
4. *Informe sobre las amenazas de ransomware (Unit 42)*, Palo Alto Networks, 20 de abril de 2021, https://start.paloaltonetworks.es/unit-42-ransomware-threat-report.html.


**Figura 1:** La extorsión cuádruple va en aumento

El auge de la «cuádruple extorsión» (figura 1) es una tendencia preocupante identificada por Unit 42 (la unidad de consultoría e inteligencia sobre amenazas de Palo Alto Networks). En la actualidad, los atacantes de ransomware suelen utilizar hasta cuatro técnicas para presionar a las víctimas para que paguen:

1. **Cifrado**: las víctimas pagan para recuperar el acceso a los datos codificados y a los sistemas informáticos afectados que dejan de funcionar porque los archivos clave están codificados.
2. **Robo de datos**: los hackers filtran información confidencial si no se paga el rescate, una tendencia que se disparó en 2020.
3. **Denegación de servicio (DoS)**: las bandas organizadas de ransomware lanzan ataques de denegación de servicio que cierran los sitios web públicos de la víctima.
4. **Acoso**: los ciberdelincuentes se ponen en contacto con clientes, socios comerciales, empleados y medios de comunicación para informarles de que la organización ha sido hackeada.

Aunque es raro que una organización sea víctima de las cuatro técnicas, en 2021 se detectó un aumento de las bandas de ransomware que optan por estrategias adicionales cuando las víctimas no pagan tras el cifrado y el robo de datos. El Informe sobre las amenazas de ransomware (Unit 42, 2021), que cubría las tendencias de 2020, señalaba la doble extorsión como una práctica emergente, y las últimas observaciones revelan que los atacantes vuelven a duplicar el número de técnicas de extorsión que utilizan.

A medida que han ido adoptando estas nuevas tácticas de extorsión, las bandas de ransomware se han ido haciendo más codiciosas. De las decenas de casos que revisaron los asesores de Unit 42 en la primera mitad de 2021, la media de los rescates exigidos fue de 5,3 millones de dólares. Esto supone un aumento del 518 % respecto a la media de 2020, que fue de 847 000 dólares.

La crisis del ransomware seguirá cobrando fuerza en los próximos meses, a medida que los grupos de ciberdelincuentes sigan perfeccionando las tácticas para coaccionar a las víctimas para que paguen y desarrollen nuevas estrategias para que los ataques sean más disruptivos.

# Preparar y prevenir

El ransomware actúa con rapidez —a veces a los pocos minutos de la infección—, por lo que resulta crucial tomar medidas e implementar controles que mitiguen o prevengan los ataques. En los dos apartados siguientes se resumen las principales recomendaciones para ambas cosas.

## Recomendaciones para mitigar los efectos de un ataque de ransomware

### Desarrollar un plan para poner en marcha un programa de concienciación de los usuarios finales.

- Puede ser difícil conseguir la aprobación para enviar recordatorios de seguridad periódicos a toda la empresa, pero los usuarios finales más inteligentes y conscientes de los riesgos de ciberseguridad sin duda sufrirán menos incidentes de ransomware.

### Revisar o validar los procesos de copia de seguridad de los servidores.

- Las copias de seguridad mal configuradas o almacenadas en una ubicación vulnerable a los riesgos pueden dar lugar a más pérdidas, económicas o de otro tipo.
- Revise los servidores de archivos críticos que alberguen recursos compartidos para los departamentos cruciales y planifique la revisión periódica del proceso de recuperación de estos servidores.

### Realizar revisiones de los privilegios de los usuarios finales.

- Designe a un delegado de confianza que desarrolle y organice un proceso de evaluación de los permisos que tienen los usuarios en las unidades de red asignadas. Siempre que sea posible, aplique el principio del mínimo privilegio para minimizar las consecuencias que puedan tener las acciones de un solo usuario.
- En el proceso de revisión, empiece por examinar los privilegios de los usuarios finales para los recursos y departamentos cruciales.
- Exija contraseñas seguras, únicas y complejas para todas las cuentas.
- Revise los permisos de las unidades de red para minimizar las consecuencias que puedan tener las acciones de un solo usuario.

### Establecer revisiones de los privilegios de los usuarios administradores.

- Audite las funciones con privilegios que utilicen los equipos responsables de los servidores, las copias de seguridad y las redes para validar que exista un nivel de acceso adecuado.
- Asegúrese de que a los administradores se les asignen cuentas normales y restringidas, independientes de sus cuentas con muchos privilegios.
- Exija a los administradores que utilicen sus cuentas con muchos privilegios solo cuando las necesiten.
- Elimine de las cuentas administrativas las asignaciones automáticas de las unidades de red, siempre que sea posible.
- Restrinja la recepción de correo electrónico en las cuentas administrativas.
- Exija la autenticación multifactor para todos los usuarios —incluidas las cuentas administrativas— y controle posibles usos anómalos.
- Exija contraseñas seguras, únicas y complejas para todas las cuentas.

### Documentar un plan de respuesta a incidentes de ransomware.

- Asegúrese de que los procesos de respuesta al ransomware están incluidos en su plan de respuesta a incidentes. Recuperarse de un ataque de ransomware requiere un proceso único para el que hay que tener un plan propio.
- Los casos en que se cifran todos los archivos de la unidad de disco de todo un departamento pueden llegar a ser bastante complejos, ya que se requiere la intervención de varios equipos: el de copias de seguridad, el de servidores de archivos, el de endpoints, el de directorios, etc. Cuanto más completa sea la planificación, más breve será el tiempo de respuesta.

## Principales recomendaciones para prevenir las infecciones de ransomware

### Aplicar enseguida los parches de software.

- Revise los procesos de aplicación de parches y la aceptación de riesgos e identifique oportunidades para eliminar obstáculos.
- Compruebe que los servicios de VPN y de intercambio de archivos estén actualizados.

### Protegerse contra las amenazas de correo electrónico.

- Configure protecciones para el correo entrante y bloquee aquellos archivos que presenten un mayor riesgo.
- Impida que los usuarios habiliten las macros bloqueando su ejecución en las aplicaciones de MS.
- Inspeccione los correos electrónicos en busca de direcciones URL maliciosas.
- Forme a los usuarios finales en técnicas de *phishing* e ingeniería social.

### Implementar un cortafuegos de nueva generación.

- Compruebe que el cortafuegos bloquee automáticamente las amenazas conocidas basándose en una fuente de amenazas de confianza que se actualice constantemente.
- Asegúrese de que el cortafuegos ofrezca funciones de sandboxing para detener las amenazas desconocidas (direcciones URL y ejecutables) antes de que lleguen al endpoint.
- Configure el cortafuegos o proxy de modo que se requiera la interacción del usuario final cuando se conecte a sitios web etiquetados como «sin categorizar» (por ejemplo, que tenga que hacer clic en un botón de «Continuar»). Muchos de estos sitios web se utilizan en campañas de *phishing* dirigidas para distribuir malware. Este proceso de dos pasos evita que determinados tipos de ransomware efectúen una llamada externa al servidor de comando y control. Si esto no sucede, es posible que sus archivos no se cifren.
- Asegúrese de que las firmas estén actualizadas con respecto a las vulnerabilidades de escritorio remoto.
- Compruebe que el cortafuegos de nueva generación incluya funciones de filtrado avanzado de URL para detectar amenazas desconocidas.

### Implementar un mecanismo de protección avanzada del endpoint.

- Asegúrese de que las medidas de protección del endpoint puedan detectar y prevenir el malware conocido y desconocido, y también los exploits conocidos y desconocidos, incluidos los de día cero.
- Incorpore la detección de malware basada en el comportamiento y utilice listas de permitidos.
- Compruebe que los sistemas de protección del endpoint estén provistos de inteligencia sobre amenazas en tiempo real procedente de fuentes internas y externas que transcienden los límites empresariales, geográficos y sectoriales.

### Restringir y gestionar el acceso externo a la red.

- El acceso directo externo a escritorios remotos debe estar deshabilitado de forma predeterminada. Cuando se requiera acceso externo, asegúrese de que todas las conexiones administrativas se realicen a través de una VPN empresarial con autenticación multifactor.
- Limite los privilegios de los usuarios siempre que sea posible, incluidos los que utilizan dispositivos personales en el trabajo.

### Conocer el entorno.

- Mantenga un inventario actualizado de todos sus activos. Valide sistemáticamente el inventario y las cuentas asociadas a cada dispositivo.
- Establezca unos patrones normales para el funcionamiento de la red y defina alertas a nivel global para aquellas actividades que no se ajusten a ellos.
- Identifique todo el tráfico de la red y bloquee todo el que sea de alto riesgo.
- Revise e inspeccione los mecanismos de protección de todos los servicios expuestos a Internet.

## Cómo ayuda Cortex XDR a prevenir, detectar y detener los ataques de ransomware

Cortex® XDR™ es una plataforma integrada de prevención, detección y respuesta basada en distintos conjuntos de datos (figura 2) que permite a su equipo de seguridad contener al instante las amenazas a la red, los endpoints y la nube desde una única consola. Los analistas podrán detener rápidamente la propagación del malware, restringir la actividad de la red hacia los dispositivos y desde ellos, así como actualizar las listas de prevención de amenazas, como los dominios peligrosos, mediante una integración perfecta con los puntos de aplicación de las políticas. Con Cortex XDR, también podrá:

- bloquear los ataques de ransomware en cada fase del ciclo de vida del ataque, desde el exploit inicial hasta el análisis de archivos y la protección basada en el comportamiento;
- encontrar ataques sigilosos gracias a la IA y al análisis transversal de datos;
- investigar rápidamente gracias al análisis de causas originales;
- contener cualquier amenaza con una respuesta coordinada.

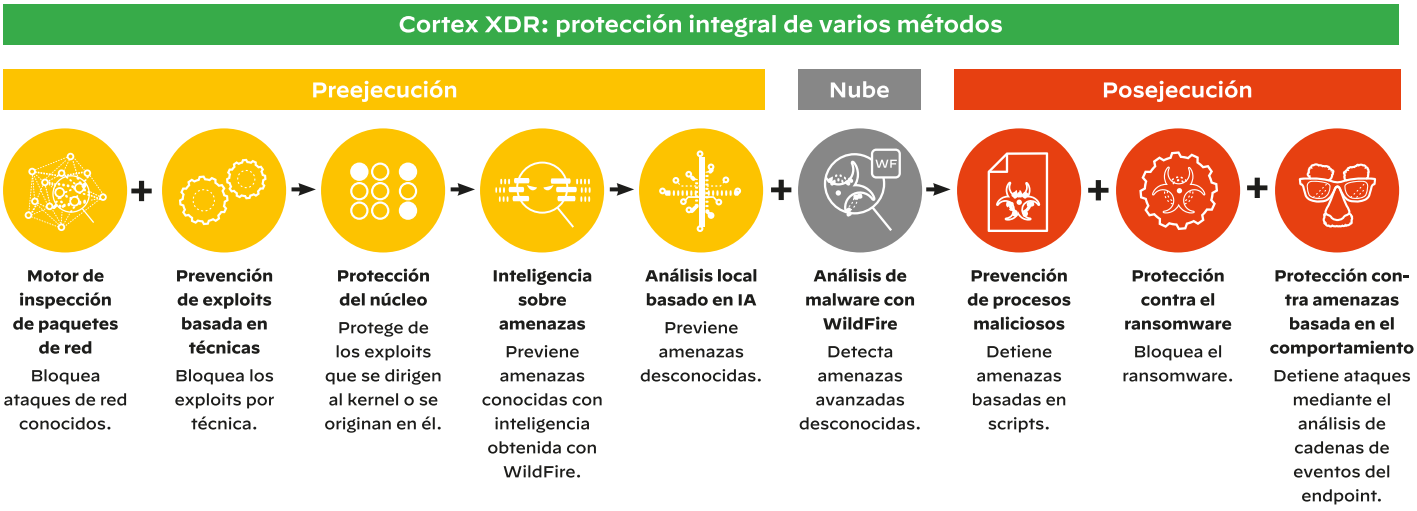


**Figura 2:** Cortex XDR incluye funciones como la búsqueda de XQL, la agrupación de alertas en incidentes o la identificación de la causa original de las alertas procedentes de cualquier fuente

## Opciones de respuesta en Cortex XDR

- **Live Terminal** para garantizar el acceso directo al endpoint incluye un gestor gráfico de tareas y archivos para ver y terminar procesos, eliminar archivos, descargar archivos, ejecutar comandos y mucho más.
- **Script Execution** para ejecutar desde nuestra consola de gestión prácticamente cualquier script de Python en un endpoint, un grupo de endpoints o en todos ellos.
- **Search and Destroy** indexa todos los archivos de los endpoints para encontrar y eliminar en tiempo real archivos maliciosos en cualquier lugar de la organización.
- **Host Restore** para recuperar un endpoint atacado.

Con nuestras sugerencias de corrección, puede eliminar el malware, restaurar los archivos a partir de la instantánea de Windows y eliminar los cambios en las claves de registro. Estas funciones se suman a las opciones de respuesta más tradicionales, como la cuarentena, el aislamiento de la red, el bloqueo de archivos y la integración con Cortex XSOAR para ofrecer una respuesta automatizada.

### Los sistemas tradicionales de protección, detección y respuesta en el endpoint no son suficientes

- No pueden identificar y bloquear los ataques avanzados a los endpoints.
- Requieren demasiados procesos manuales.
- Ofrecen una visión limitada del entorno, centrada solo en los endpoints.
- Dependen de analistas expertos para investigar las alertas manualmente.
- Presentan carencias a la hora de detectar las amenazas nuevas y avanzadas.

# Cinco medidas imprescindibles en caso de sufrir un ataque

1. **Aislar la red.** Inhabilite todos sus NIC virtuales.
2. **Prestar atención a dónde puede estar almacenada la información sobre el ataque antes de reiniciar.** A veces, la clave de cifrado y demás información relativa al ataque puede encontrarse en la memoria.
3. **Verificar las copias de seguridad de los datos pertinentes** y determinar el riesgo global para la organización si no se paga el rescate.
4. **Comprobar si existe una herramienta de descifrado consultado la página** https://www.nomoreransom.org/es/index.html.
5. Llamar a un equipo IR como el de Entel Ocean. Nosotros contamos con un centro de inteligencia de más de 50 especialistas que te ayudarán a desarrollar y profundizar tus estrategias de seguridad en tiempo récord, brindándote asesoría para la protección y gestión de riesgos y para cumplir con las normativas vigentes, entre otros beneficios. Descubre nuestros servicios de ciberseguridad y protege tu empresa de las ciberataques.

### Para más información:

**Ve a nuestro** sitio web
**Descarga nuestro** Datasheet
Ver video

**¿Estás considerando implementar nuestros servicios de ciberseguridad y proteger tu empresa de los ciberataques? Ponte en contacto con nosotros**

**Hablemos**

paloalto NETWORKS | ocean