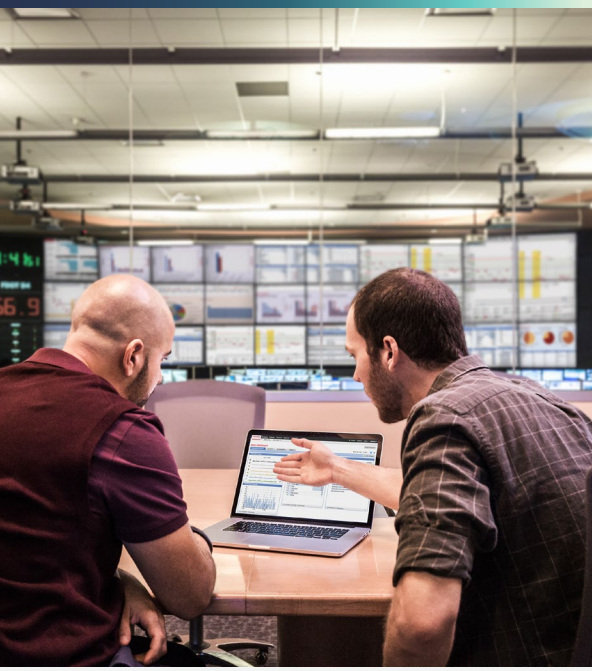
Resumen



## Ventajas

- **Reduzca el riesgo** de infecciones de ransomware con una seguridad que puede bloquear las amenazas antes de que intenten arraigarse.
- **La protección inmediata** contra el ransomware le permite centrarse en dirigir su empresa.
- **Las defensas integradas por capas** le ofrecen una visibilidad y una capacidad de respuesta inigualables desde la capa de DNS, pasando por la red, hasta el terminal.
- **Segmentación dinámica** para mantener al ransomware acorralado en la red.
- **Información líder del sector** distribuida por Cisco Talos Security Intelligence and Research Goup.

# Cisco Ransomware Defense

## El auge del ransomware

El ransomware es software malicioso, o malware, que cifra la información contenida en el ordenador de una persona, como documentos, fotos y música. No liberará estos archivos hasta que el usuario pague una tarifa (o rescate) para desbloquearlos y recuperarlos.

El ransomware se ha convertido rápidamente en el tipo de malware más rentable de la historia y está en camino de generar un mercado de 1000 millones de dólares anuales.

Normalmente, se abre camino hacia los ordenadores o redes a través de la Web o el correo electrónico. En un sitio web, el ransomware puede infiltrarse a través de anuncios infectados que pueden distribuir malware, conocidos como "malvertising". Los usuarios acceden a sitios con anuncios maliciosos que descargan malware automáticamente o los redirigen a exploit kits. En el correo electrónico, el ransomware utiliza mensajes de suplantación de identidad o spam para introducirse. Los usuarios solo tienen que hacer clic en los enlaces del correo electrónico de suplantación de identidad o spam, o abrir los archivos adjuntos, para que el ransomware se descargue y llame a su servidor de comando y control.

El ransomware también puede controlar los sistemas mediante exploit kits. Los exploit kits son kits de software diseñados para identificar las vulnerabilidades del software en los sistemas finales. A continuación, cargan y ejecutan el código malicioso, como el ransomware, en dichos sistemas vulnerables.

En el futuro, el ransomware no solo se dirigirá a usuarios particulares, sino también a redes completas. Con más métodos de propagación semiautomáticos, los autores del ransomware aprovecharán las oportunidades para vulnerar una red y moverse de forma lateral para controlar las franjas de la red y maximizar el impacto y la probabilidad de recibir los pagos.

## Reduzca el riesgo de ransomware con una seguridad más eficaz

Dado que el ransomware puede penetrar en las organizaciones de diversas formas, reducir el riesgo de infecciones de ransomware requiere un enfoque que se base en un portafolio de productos, más que en un único producto. El ransomware debe evitarse en la medida de lo posible, detectarse si accede a los sistemas y contenerse para limitar los daños.

Cisco® Ransomware Defense recurre a la arquitectura de seguridad de Cisco para proteger las empresas mediante defensas que abarcan desde las redes hasta los terminales, pasando por la capa de DNS y el correo electrónico. Además, está respaldado por Talos, el equipo de investigación de amenazas líder del sector, para obtener la mayor capacidad de respuesta frente al ransomware.

"Hemos cubierto un gran riesgo en el vector de ataque de la Web del ransomware y hemos mejorado significativamente nuestra experiencia de usuario en relación con la conectividad a Internet".

Octapharma

La solución comprende los siguientes componentes:

- **Cisco Umbrella** protege los dispositivos tanto dentro como fuera de la red corporativa. Bloquea las solicitudes de DNS antes de que un dispositivo pueda incluso conectarse a sitios maliciosos que albergan ransomware.
- **La protección frente a malware avanzado (AMP) de Cisco para terminales** bloquea los archivos de ransomware para evitar que se abran en los terminales.
- **Cisco Email Security con protección frente a malware avanzado (AMP)** bloquea los correos electrónicos de spam y suplantación de identidad así como los archivos adjuntos y las URL de correos electrónicos maliciosos. La tecnología AMP es la misma que la que se aplica en los terminales, pero se implementa en la puerta de enlace del correo electrónico.
- **El firewall de última generación Cisco Firepower** con protección frente a malware avanzado (AMP) y tecnología de sandboxinThreat Grid bloquea las amenazas y callbacks de comando y control conocidas, a la vez que proporciona análisis dinámicos de las amenazas y el malware desconocido.
- **Cisco ISE a través de la red de Cisco** para segmentar de forma dinámica su red, de forma que el acceso a los servicios y a las aplicaciones siga siendo muy seguro y el ransomware no pueda propagarse de forma lateral.
- **Los servicios de seguridad Cisco Security Services** proporcionan una clasificación inmediata en caso de respuesta a incidentes. También simplifican las implementaciones de AMP, NGFW y otros productos.

## Siguientes pasos

Mantenga su empresa centrada en sus tareas poniéndose en contacto con su representante de ventas de Cisco para obtener más información sobre Cisco Ransomware Defense.



C45-737465-00 07/16