SOPHOS

Prácticas recomendadas de protección para endpoints para bloquear el ransomware

Guía práctica de configuración de su solución para endpoints a fin de proporcionar una protección óptima.

Monográficos de Sophos. Octubre de 2024

Introducción

El ransomware figura entre las ciberamenazas más importantes, pues sus consecuencias son de gran alcance y a menudo catastróficas. El 59 % de los participantes en la encuesta El estado del ransomware 2024 de Sophos informaron que su organización se vio afectada por el ransomware en el año anterior. En el 70 % de estos incidentes, los atacantes cifraron los datos.

En general, el coste medio para remediar un ataque de ransomware ascendió a la demoledora cifra de 2,73 millones USD, lo que supone un aumento del 50 % con respecto al año anterior. Además, más de un tercio (34 %) de las organizaciones tardaron más de un mes en recuperarse de los ataques, lo que subraya la creciente complejidad y gravedad de estos incidentes.

El hecho de que los plazos de recuperación se alarguen pone de manifiesto la necesidad de adoptar medidas de respuesta más exhaustivas. Esta creciente complejidad también ejerce una presión considerable sobre los equipos de seguridad internos: el 95 % de las organizaciones afirman tener dificultades para llevar a cabo las tareas esenciales de las operaciones de seguridad[1].

Dado que el aumento de los costes, de los tiempos de recuperación y de la presión sobre los equipos de seguridad convierten al ransomware en una tremenda amenaza para la continuidad de las empresas, estos resultados subrayan la necesidad urgente de que las organizaciones refuercen sus defensas y estrategias de recuperación frente al ransomware Una solución de protección de endpoints bien configurada es una de las defensas más eficaces contra el ransomware. Este monográfico profundiza en la mecánica de los ataques de ransomware, las estrategias para prevenirlos y las prácticas recomendadas para optimizar la protección para endpoints y garantizar la máxima seguridad.

Cómo se despliegan los ataques de ransomware

Hay muchos ciberdelincuentes y muchos tipos de ataques de ransomware. Algunos son muy específicos, mientras que otros son oportunistas. A menudo, los adversarios escanean las redes en busca de puntos débiles o vulnerabilidades que les permitan acceder al entorno de una empresa. Valga como ejemplo la observación siguiente de una banda de ransomware que atacó una organización educativa canadiense:

> *"Teníais una vieja vulnerabilidad Log4j crítica sin parchear en Horizon; es así como pudimos acceder en un principio. Fue un escaneado masivo, no pretendíamos lanzar un ataque dirigido".*

Esta observación también pone de relieve la explotación habitual por parte de los adversarios de las vulnerabilidades no parcheadas, que fue la principal causa de los ataques de ransomware en 2024.[2]

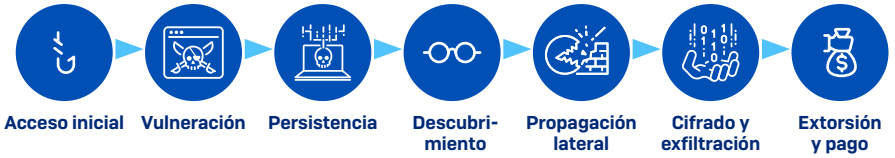
Gran parte del aumento de los ataques de ransomware en los últimos años puede atribuirse al creciente modelo de ransomware como servicio (RaaS). Con RaaS, un grupo de ciberdelincuentes crea ransomware y lo alquila a otros adversarios. Este enfoque reduce la barrera de entrada y hace que el ransomware sea accesible a más adversarios que nunca.

Una vez los adversarios se encuentran dentro de los entornos de sus víctimas, frecuentemente pasan muchos días, semanas o meses explorando la red, aumentando los privilegios, exfiltrando datos e instalando malware. En 2023, el tiempo medio de permanencia en los ataques de ransomware fue de 6 días[3]. Esto ofrece a los responsables de la seguridad una oportunidad para identificar y detener a los intrusos antes de un ataque.

1 El problema de la falta de conocimientos de ciberseguridad en las pymes - Sophos

2 El estado del ransomware 2024 - Sophos
3 Un aparente mar en calma: Informe de Sophos sobre adversarios activos para el primer semestre de 2024 - Sophos

Este es un ejemplo del ataque de ransomware típico:



Cabe destacar que los adversarios atacan estratégicamente a las organizaciones en momentos en los que es menos probable que se les detecte. Los ataques de ransomware suelen producirse los viernes o los sábados, aprovechando que durante el fin de semana suele haber menos personal de TI pendiente de los sistemas.

Según el análisis realizado por los expertos en respuesta a incidentes de Sophos X-Ops, el 43 % de los ataques de ransomware en 2023 se programaron para esos días, y el 91 % de ellos se iniciaron fuera del horario normal de oficina (de 8:00 a 18:00 h de lunes a viernes) en la zona horaria de la víctima, para así aprovechar los periodos en los que la probabilidad de detección y respuesta era menor[4].

Ransomware remoto

El Informe de protección digital de Microsoft 2023 afirma que alrededor del 60 % de los ataques de ransomware perpetrados por humanos implican el cifrado remoto. El cifrado remoto, también conocido como ransomware remoto, se produce cuando un endpoint vulnerado se utiliza para cifrar los datos de otros dispositivos de la misma red.

Un factor clave que influye en el uso cada vez más extendido de este enfoque es su escalabilidad: un endpoint no administrado o mal protegido puede exponer a toda la organización a un cifrado remoto malicioso, aunque otros dispositivos tengan instaladas soluciones de seguridad avanzadas.

Las organizaciones deben tomar conciencia de la amenaza que suponen los ataques de ransomware remoto, ya que no todas las soluciones de seguridad para endpoints pueden proteger eficazmente contra ellos.

4 Detenga a los adversarios activos: Lecciones desde la primera línea de combate cibernética - Sophos

¿Protocolo de escritorio remoto o protocolo de despliegue de ransomware?

El protocolo de escritorio remoto (RDP) tuvo un papel importante en el 90 % de los ciberataques investigados por el equipo de respuesta a incidentes de Sophos en 2023, lo que representa una subida frente al 83 % del año anterior[5].

El RDP y las herramientas de uso compartido del escritorio como Computación virtual en red (VNC) son útiles para la gestión remota del sistema, pero sin unas medidas de protección adecuadas, los ciberdelincuentes los explotan para aumentar privilegios, robar credenciales, moverse lateralmente, instalar puertas traseras, crear cuentas falsas y eludir la detección.

Es fundamental evitar que los adversarios utilicen el RDP para el acceso externo, el acceso interno y la propagación lateral. Aunque las organizaciones han progresado a la hora de garantizar que el RDP no se exponga externamente, los adversarios lo utilizan de forma generalizada para moverse lateralmente dentro de una organización.

5 Un aparente mar en calma: Informe de Sophos sobre adversarios activos para el primer semestre de 2024 - Sophos

Prácticas recomendadas de TI para protegerse del ransomware

Protegerse contra el ransomware y otras amenazas requiere algo más que contar con las últimas soluciones de seguridad. Unas buenas prácticas de seguridad TI, incluyendo la formación periódica de los empleados, son fundamentales. Aunque no es una lista completa, asegúrese de seguir estas prácticas recomendadas.

1. Aplique los parches con prontitud y frecuencia

¿Sabía que...
Aunque todos los ataques de ransomware conllevan resultados negativos, los que comienzan con la explotación de vulnerabilidades sin parchear resultan especialmente devastadores. Las organizaciones afectadas por ataques que empezaron de esta forma registraron costes de recuperación 4 veces superiores y tiempos de recuperación más largos, en comparación con las empresas atacadas a través de credenciales vulneradas.

La explotación de vulnerabilidades sin parchear fue la principal causa de los ataques de ransomware en 2024[6]. El malware y los adversarios explotan las vulnerabilidades de seguridad de las aplicaciones más populares. Cuanto antes aplique los parches en sus endpoints, servidores, dispositivos móviles y aplicaciones, menor será la cantidad de brechas que los adversarios pueden explotar.[7]

2. Utilice contraseñas seguras

Parece irrelevante, pero no lo es. Una contraseña poco segura y predecible puede dar a los hackers acceso a su red en cuestión de segundos. Recomendamos que las contraseñas sean únicas, que consten de al menos 12 caracteres, que utilicen una combinación de mayúsculas y minúsculas y signos de puntuación aleatorios, dE.e5taM4Nera!

3. Active la autenticación multifactor (MFA)

La MFA ofrece una capa adicional de seguridad después del primer factor, que suele ser una contraseña. Es fundamental habilitar la MFA en todas las aplicaciones y servicios que la admiten. Con frecuencia, los adversarios compran credenciales válidas en la Web Oscura o tratan activamente de obtener credenciales una vez que están dentro del entorno.

La MFA supone un obstáculo adicional para un adversario y le impide autenticarse como un usuario válido sin superar un desafío. Por último, cuando las aplicaciones las admitan, utilice claves de acceso a prueba de phishing.

4. Regule el acceso interno y externo a la red

No deje los puertos de red expuestos. Bloquee el acceso RDP de su empresa y otros protocolos de gestión remota. Asegúrese de que los usuarios remotos utilizan una solución Zero Trust Network Access (ZTNA) para acceder a aplicaciones, servicios y otros recursos de la organización.

5. Supervise los derechos de administrador

Revise constantemente los derechos de administrador local y de dominio. Sepa quiénes disponen de ellos y quiénes no los necesitan. No permanezca conectado como administrador más tiempo del necesario.

6. Realice copias de seguridad periódicas en varias ubicaciones y practique con regularidad la restauración de datos

En nuestra encuesta El estado del ransomware 2024, el 68 % de los directores de TI cuyos datos se cifraron lograron restaurarlos mediante copias de seguridad. Realice regularmente copias de seguridad de sus datos en varias ubicaciones, utilizando la MFA para proteger las copias de seguridad en la nube. Practique con regularidad la restauración de datos a partir de las copias de seguridad para garantizar una recuperación sin complicaciones. Supervise la actividad sospechosa para proteger las copias de seguridad de posibles amenazas.

7. Elimine las aplicaciones innecesarias

Los adversarios utilizan las aplicaciones instaladas habitualmente con fines maliciosos. Este enfoque, denominado "vivir de la tierra" (técnica LOL, por sus siglas en inglés), hace más difícil diferenciar el uso legítimo de la actividad maliciosa. Si un usuario no necesita una aplicación para hacer su trabajo, considere detenidamente si debe instalarla. En caso de duda, no la instale.

8. Identifique dispositivos desprotegidos en la red

Los adversarios buscan dispositivos sin protección para endpoints para pasar desapercibidos en su entorno y librarse de tener que superar desafíos de autenticación. Estos dispositivos desprotegidos pueden utilizarse en ataques de ransomware remotos.

6 El estado del ransomware 2024 - Sophos
7 Vulnerabilidades sin parchear: el vector de ataque de ransomware más arrollador - Sophos

Prácticas recomendadas para la protección de endpoints

Un método eficaz para protegerse de los ataques de ransomware es una solución de protección para endpoints, de detección y respuesta para endpoints (EDR) o de detección y respuesta ampliadas (XDR) con tecnologías avanzadas de prevención y funciones de búsqueda de amenazas.

Los errores de configuración de las herramientas de seguridad se consideran el principal riesgo de ciberseguridad para las organizaciones[8]. Los parámetros de políticas mal configurados, las exclusiones y otros factores pueden comprometer la postura de seguridad. Asegúrese de que la protección para endpoints está configurada correctamente para ofrecer la máxima protección.

Por lo tanto, aconsejamos que siga estas prácticas recomendadas para proteger sus dispositivos endpoint del ransomware:

1. Habilite todas las políticas y funciones recomendadas

Parece obvio, pero es una manera segura de beneficiarse de la mejor protección de su solución de seguridad para endpoints.

Las políticas y los ajustes están diseñados para detener amenazas específicas, y comprobar periódicamente que todas las opciones de protección están activadas garantiza que los endpoints están protegidos frente al ransomware actual y emergente. Compruebe que estén activadas las funciones que detectan las técnicas usadas en los ataques sin archivos y las tecnologías de análisis de comportamientos. Además, le recomendamos que:

A) Active la protección contra manipulaciones

Esto impide la modificación o la eliminación no autorizada del software de protección para endpoints. Una de las primeras maniobras de los adversarios tras acceder a un sistema es intentar desactivar o eliminar la protección para endpoints.

B) Active un registro de nivel forense (a ser posible en la nube)

Si sufre un ataque, querrá saber qué ha pasado para poder evitar que vuelva a ocurrir. Sin embargo, los adversarios suelen borrar los registros del sistema para ocultar sus actividades, eliminando las pruebas forenses que ayudarían a comprender el ataque. Además, es posible que deje de tener acceso a su dispositivo. Disponer de un registro de la actividad en la nube asegura que pueda conservar el acceso a la información crítica.

C) Asegúrese de que las actualizaciones del producto y las de contenido de la protección para endpoints están habilitadas

Para seguir el ritmo del panorama de amenazas en constante evolución y protegerse de las amenazas emergentes, es de vital importancia actualizar periódicamente los productos de seguridad con nuevos datos. Desactivar las actualizaciones del producto y las de contenido degradará su protección con el tiempo.

2. Revise periódicamente sus exclusiones

Las exclusiones evitan que se analicen los directorios y los tipos de archivo de confianza en busca de malware. Se usan a veces para reducir retrasos en el sistema y minimizar el riesgo de falsos positivos en las alertas de seguridad.

Con el tiempo, una lista creciente de exclusiones crea brechas de seguridad que los adversarios podrían explotar. El malware que consigue entrar en los directorios excluidos, tal vez movidos por error por un usuario, podría lograr su objetivo.

Compruebe regularmente su lista de exclusiones en la configuración de sus políticas y elimine todas las que pueda. Para las que no pueda quitar, asegúrese de que sean lo más específicas posibles. Por ejemplo, en vez de excluir el directorio o la unidad de una base de datos, excluya solo archivos específicos con su ruta completa. Esto evita que el malware pueda superar su seguridad y ejecutarse desde la misma carpeta.

3. Active la MFA en su consola de seguridad

De este modo, garantiza un acceso seguro a la plataforma que gestiona su protección para endpoints y otros controles de seguridad. Esto impide que los adversarios cambien deliberadamente su configuración o desactiven/eliminen la protección, lo que puede dejar sus endpoints y servidores expuestos a ataques.

4. Mantenga unas buenas prácticas y una buena higiene de TI

Evaluar regularmente su higiene de TI garantiza que sus endpoints y el software instalado funcionen con la máxima eficiencia. Esto mitiga sus riesgos de ciberseguridad y puede ahorrarle tiempo al remediar incidentes futuros.

La implementación de un programa para mantener la higiene de TI es especialmente crítica para la protección contra los ataques de ransomware y otras amenazas de ciberseguridad. Por ejemplo, garantizar que el RDP se ejecuta solo donde se necesita y se espera, comprobar periódicamente si hay problemas de configuración, supervisar el rendimiento de los dispositivos y eliminar los programas no deseados o innecesarios. Una revisión de la higiene de TI puede poner de manifiesto la necesidad de actualizar las aplicaciones de software. También es una forma segura de garantizar que se realizan copias de seguridad de sus datos regularmente.

8 Afrontar la falta de conocimientos de ciberseguridad en las pymes - Sophos

5. Busque adversarios activos en el entorno de forma proactiva

En el panorama de amenazas actual, los adversarios son más astutos que nunca y frecuentemente despliegan herramientas legítimas y credenciales robadas para evitar la detección. Para identificar y detener estos ataques que "viven de la tierra", es fundamental buscar de forma proactiva las amenazas avanzadas y los adversarios activos. Una vez encontrados, también debe ser capaz de tomar las medidas adecuadas para poder detenerlos rápidamente.

Tecnologías como la detección y respuesta para endpoints (EDR) y la detección y respuesta ampliadas (XDR) ofrecen funciones de búsqueda, investigación y neutralización de amenazas para su equipo de seguridad interno. Sin embargo, como los adversarios suelen iniciar sus ataques fuera del horario de oficina, es posible que su equipo de seguridad no esté disponible para frenarlos. Muchas organizaciones tienen dificultades para mantener una cobertura las 24 horas que les permita defenderse contra los ataques avanzados de ransomware, y esa es la razón por la que los servicios de detección y respuesta gestionadas (MDR) son esenciales para muchas de ellas.

Tecnologías de seguridad multicapa para protegerse del ransomware

El dicho "más vale prevenir que curar" pone de relieve que detener un problema a tiempo es más fácil que reparar los daños más tarde. Adoptar un enfoque de seguridad TI por capas, en el que varias tecnologías trabajan juntas para ofrecer protección y visibilidad, es muy eficaz para proteger a su organización frente al ransomware. Empezando por la protección para endpoints, las organizaciones pueden ir añadiendo más capas a medida que cambien sus necesidades, mejorando la protección y la visibilidad con el tiempo.

Ejemplos:

- **Un firewall** identifica y bloquea el tráfico de red sospechoso e impide que las amenazas entren en el entorno. El firewall tiene visibilidad sobre el tráfico de red que entra y sale de una organización. No tiene visibilidad sobre el tráfico de red dentro del entorno.
- **Un producto de detección y respuesta de red (NDR)** puede detectar dispositivos desprotegidos e identificar a los adversarios que se mueven lateralmente en la red. NDR proporciona visibilidad sobre el tráfico interno de la red que un firewall no puede ver.
- **Una plataforma XDR** ofrece funciones de búsqueda, investigación y neutralización de amenazas. También puede integrarse con sus otras soluciones de seguridad TI, aportando visibilidad a través de todos los controles de seguridad desde una única plataforma.
- **Un servicio de MDR** proporciona monitorización y búsqueda de amenazas 24/7 suministrada por expertos especializados en detectar y responder a los ciberataques que las soluciones tecnológicas por sí mismas no pueden evitar. Un servicio de MDR debe ofrecer una respuesta a incidentes integral para interrumpir, contener y eliminar por completo a los adversarios sin costes adicionales. También debe integrarse con sus herramientas de ciberseguridad existentes para obtener una visibilidad completa de todo su entorno. MDR ofrece el nivel máximo de protección contra los ataques avanzados de ransomware perpetrados por humanos.
- **Una solución de gestión de la superficie de ataque externa (EASM) o de gestión de vulnerabilidades (VM)** puede utilizarse para identificar y priorizar las vulnerabilidades. Así podrá identificar y aplicar los parches que falten antes de que los adversarios puedan explotarlos.

Sophos protege contra el ransomware

Sophos Endpoint adopta un enfoque integral de la seguridad centrado en la prevención para bloquear las amenazas sin depender de una única técnica. Utiliza tecnologías sofisticadas que bloquean la más amplia variedad de ataques, entre ellas:

- **Protección hermética contra el ransomware**: protege de los ataques de ransomware local y remoto, incluidas las nuevas variantes. Detiene el cifrado malicioso en tiempo real y revierte automáticamente los archivos afectados a su estado original, lo que minimiza el impacto en la empresa.
- **Tecnología antiexploits**: protege ante los ataques sin archivos y los exploits de día cero al detener las técnicas utilizadas por los adversarios en toda la cadena de ataque.
- **Protección adaptativa contra ataques**: protección dinámica pionera en el sector que se adapta en respuesta a los adversarios activos y los ataques manuales directos. El refuerzo de las defensas, activado dinámicamente, impide que los adversarios lleven a cabo más acciones al minimizar la superficie de ataque e interrumpir el ataque.

Sophos Endpoint es fácil de configurar y gestionar. Basta con instalar Sophos Endpoint y ponerse en marcha. Las tecnologías de protección recomendadas están activadas por defecto para que disponga inmediatamente de la máxima protección sin necesidad de realizar ajustes. Si lo necesita, también puede disponer de control granular.

Sophos Endpoint se gestiona a través de **Sophos Central,** la plataforma de gestión de ciberseguridad en la que más confía el mundo. Esta potente plataforma de administración de ciberseguridad basada en la nube unifica todas las soluciones de seguridad next-gen de Sophos e impone la MFA para el acceso.

Los clientes de Sophos gestionan su protección para endpoints a través de Sophos Central y se benefician de la función "Verificar estado de cuenta". Esta identifica las desviaciones de la postura de seguridad en políticas y exclusiones, y otros errores de configuración de alto riesgo, lo que permite a los administradores solucionar los problemas con un solo clic.

Sophos XDR: herramientas de búsqueda proactiva de amenazas e higiene de TI

Sophos XDR es una plataforma unificada de detección y respuesta que se basa en el enfoque centrado en la prevención de Sophos Endpoint. Le permite detectar, investigar y responder rápidamente a las amenazas de varias fases, en todos los vectores de ataque claves.

Las tecnologías de Sophos, totalmente integradas en la plataforma XDR de Sophos, funcionan juntas para ofrecer los mejores resultados de ciberseguridad posibles. Asimismo, obtendrá más rentabilidad de sus productos de ciberseguridad existentes al disponer de integraciones preconfiguradas con un amplio ecosistema de soluciones de seguridad de terceros para endpoints, firewalls, redes, correo electrónico, identidad, productividad, la nube y copias de seguridad y recuperación.

Sophos XDR proporciona herramientas y funciones diseñadas para maximizar la eficiencia de los analistas de seguridad y administradores de TI.

- Las detecciones priorizadas por IA en todas las superficies de ataque claves ayudan a identificar la actividad sospechosa que requiere atención inmediata.
- Las detecciones y los casos se asignan automáticamente a las tácticas de MITRE ATT&CK, lo que le permite identificar fácilmente las lagunas en sus defensas.
- Las acciones automatizadas como la finalización de procesos, la reversión del ransomware y el aislamiento de la red frenan las amenazas rápidamente, lo que le ahorrará un tiempo muy valioso. Las funciones de IA generativa centrada en resultados permiten a los analistas de seguridad neutralizar a los adversarios más rápidamente, lo que aumenta la eficacia de los analistas y la confianza de la empresa.

Sophos MDR: detección y respuesta gestionadas 24/7

Sophos MDR es un servicio de seguridad gestionada 24/7 prestado por expertos altamente cualificados que gestionan la protección frente a nuevas amenazas y adversarios activos avanzados en su nombre. El servicio Sophos MDR ofrece la protección definitiva contra el ransomware.

Con el nivel de servicio Sophos MDR Complete, se beneficiará de una respuesta a incidentes integral ilimitada, sin topes ni costes adicionales. Nuestros expertos pueden ejecutar un gran número de acciones de respuesta en su nombre para interrumpir, contener y neutralizar por completo al adversario de forma remota.

Al igual que Sophos XDR, Sophos MDR integra y recopila telemetría de todos los productos de Sophos y se integra con la misma amplia gama de productos de seguridad de terceros para aumentar la visibilidad y la protección en todo su entorno.

Sophos Incident Response Services Retainer: un servicio de respuesta a incidentes bajo demanda

Contar con un equipo de respuesta a incidentes antes de que los adversarios ataquen es la única forma de ahorrar tiempo, reducir costes y mitigar el impacto de una filtración (por ejemplo, que los adversarios desplieguen ransomware).

Sophos Incident Response Services Retainer es una suscripción anual a un equipo de élite bajo demanda formado por expertos en respuesta a incidentes que intervendrán rápidamente en su entorno para interrumpir, contener y eliminar completamente a cualquier adversario activo. También incluye recursos críticos de preparación ante incidentes para mejorar la postura de seguridad de su organización y reducir la probabilidad de filtraciones.

Nota: no es necesario contratar Sophos Incident Response Services Retainer si se suscribe al nivel de servicio Sophos MDR Complete, que incluye de serie una respuesta a incidentes integral.

Sophos Managed Risk: servicio de gestión de vulnerabilidades y de la superficie de ataque externa

Las vulnerabilidades sin parchear son la causa principal de los ataques de ransomware, por lo que es crucial identificar, investigar y priorizar las exposiciones de alto riesgo en todo el entorno antes de que se conviertan en un problema. Sophos Managed Risk, basado en la tecnología líder del sector de Tenable, le ayuda a conseguirlo.

Con **Sophos Managed Risk**, nuestros experimentados analistas identifican vulnerabilidades de ciberseguridad de máxima prioridad y posibles vectores de ataque en su entorno, de forma que se puedan tomar medidas para evitar ataques antes de que afecten a su negocio.

Conclusión

El ransomware sigue evolucionando y sigue resultando eficaz como método de coacción para incitar a las organizaciones afectadas a pagar un rescate. Su objetivo es impedir que los adversarios entren en su organización y detectarlos y expulsarlos rápidamente si lo hacen. Siga las prácticas recomendadas de TI y de seguridad para endpoints, no deje de formar a los usuarios finales y permanezca atento a las amenazas y los adversarios en su entorno. Un enfoque a la ciberseguridad por capas y centrado en la prevención, con detección y respuesta 24/7, ofrece a su organización la mejor oportunidad de protegerse frente al ransomware y las amenazas más recientes.

Para descubrir cómo Sophos puede ayudarle a optimizar sus defensas contra el ransomware, hable con un asesor o visite es.sophos.com

2024-10-01 (WP-NP)

SOPHOS