cpl.thalesgroup.com

THALES
Building a future we can all trust

Soluciones de Thales para la prevención de ataques de ransomware

Mapeo de las soluciones de Thales con el marco de ciberseguridad del NIST y la guía de prevención de ransomware

Los ataques de ransomware han sido un problema durante años, pero recientemente se han vuelto mucho más dañinos, con delincuentes que atacan de todo, desde infraestructura crítica hasta hospitales y minoristas, y exigen decenas de millones de dólares en rescate. Hoy, con los líderes mundiales discutiendo estos ataques en cumbres de alto perfil, las agencias gubernamentales están asumiendo un papel activo en la educación y el suministro de recursos para que las empresas y organizaciones se protejan de los ataques.

Orientación del NIST para prevenir ataques de ransomware

El Centro Nacional de Excelencia en Ciberseguridad (NCCoE) bajo los auspicios del Instituto Nacional de Estándares y Tecnología (NIST) publicó una guía sobre la identificación y protección de activos contra ransomware. La Publicación especial de ciberseguridad (SP) 1800-25 establece los pasos para tener una estrategia integral en torno a la protección de activos. También muestra que no existe una fórmula mágica para abordar la amenaza del ransomware.

Soluciones de Thales para la prevención de ransomware

Las soluciones de gestión de acceso y seguridad de datos de Thales proporcionan algunos de los componentes más esenciales del marco de ciberseguridad propuesto por el NIST para proteger a las organizaciones contra el ransomware. La cartera líder en la industria de Thales brinda a las organizaciones la capacidad de:

- Descubrir datos confidenciales y clasificarlos según el riesgo
- Implementar un control de gestión del acceso e identidad robusto
- Proteger y controlar los datos confidenciales en reposo y en tránsito mediante el cifrado y la tokenización
- Supervisar la seguridad de los datos para una reparación inteligente

A continuación, se muestra un resumen de cómo nuestras soluciones se corresponden con el marco de ciberseguridad del NIST y la guía sobre el ransomware:

Mapeo de las soluciones de Thales con el marco de ciberseguridad del NIST y la guía sobre el ransomware

Categoría	Requisito	Soluciones de Thales
IDENTIFICAR **Evaluación de riesgos (ID.RA)**	ID.RA-1: Las vulnerabilidades de los activos se identifican y documentan.	**CipherTrust Data Discovery and Classification** identifica con eficacia los datos confidenciales regulados (tanto estructurados como no estructurados) en todos los almacenamientos de datos, ya sean en la nube, en macrodatos o en almacenes de datos tradicionales. Un único panel permite comprender los datos confidenciales y sus vulnerabilidades, lo que permite tomar mejores decisiones sobre cómo cerrar las brechas de seguridad, priorizar las acciones de remediación y asegurar su transformación en la nube y el intercambio de datos con terceros.
PROTEGER **Control de acceso (PR.AC)**	PR.AC-1: Las identidades y credenciales se emiten, administran, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados. PR.AC-3: Se gestiona el acceso remoto. PR.AC-4: Se gestionan los permisos y autorizaciones de acceso, incorporando los principios de mínimo privilegio y separación de funciones.	**SafeNet Trusted Access ofrece una gestión de acceso centralizada** que les permite a las organizaciones aplicar políticas de autenticación coherentes en todas las plataformas al automatizar y simplificar la implementación y la gestión de un estado distribuido de tokens, al tiempo que asegura un amplio espectro de recursos, ya sean locales, basados en la nube o virtualizados. **SafeNet Trusted Access también proporciona autenticación comercial de múltiples factores lista para usar y con la** más amplia gama de métodos de autenticación y factores de forma. Esto les permite a los clientes abordar numerosos casos de uso, niveles de garantía y vectores de amenazas con políticas unificadas administradas de forma centralizada, administradas desde un back-end de autenticación entregado en la nube o localmente. **El cifrado transparente de CipherTrust proporciona controles de acceso detallados** a los datos críticos de su empresa, que definen quién tiene acceso a archivos/carpetas protegidos específicos y qué operaciones pueden realizar. • Evite que los usuarios administrativos aprovechen sus privilegios para obtener acceso de lectura a archivos o bases de datos confidenciales. • Coloque políticas estrictas de control de acceso alrededor de los archivos de respaldo y cifre las copias de respaldo para evitar la filtración de datos. • Implemente la separación de tareas de modo que los usuarios de la base de datos puedan obtener acceso de lectura/escritura, mientras que el software de respaldo solo tenga acceso de lectura a la misma base de datos.

Categoría	Requisito	Soluciones de Thales
PROTEGER **Seguridad de los datos (PR.DS)**	PR.DS-1: Los datos en reposo están protegidos.	**La plataforma** de seguridad de datos CipherTrust unifica el descubrimiento, la clasificación, la protección de datos y los controles de acceso granulares sin precedentes con una gestión de claves centralizada, todo en una única plataforma. Esto se traduce en una reducción en los recursos dedicados a las operaciones de seguridad de datos, controles de cumplimiento omnipresentes y una reducción significativa del riesgo en toda su empresa. • **CipherTrust Transparent Encryption** ofrece cifrado de datos en reposo, controles a usuarios con acceso a información privilegiada y un registro detallado de auditoría del acceso a los datos sin necesidad de realizar cambios en las aplicaciones existentes. Les permite a las organizaciones de TI configurar políticas para evitar que los procesos fraudulentos y los usuarios no autorizados cifren sus datos más confidenciales y evita la exposición de los datos confidenciales tras su exfiltración, protegiendo así a las organizaciones de los ataques de ransomware. Los agentes protegen los datos en archivos, volúmenes y bases de datos en servidores físicos y virtuales en la nube y en macrodatos basados en sistemas operativos de Windows, AIX y Linux. • **CipherTrust Application Data Protection** ofrece funciones de cifrado como administración de claves, firmas, métodos de dispersión y servicios de cifrado a través de las API, para que los desarrolladores puedan proteger los datos con facilidad en el servidor de la aplicación o el nodo de los macrodatos. • **CipherTrust Tokenization** se encuentra disponible con y sin repositorio, y contribuye a reducir el coste y la complejidad de cumplir con las normativas en materia de seguridad de datos (como PCI-DSS). • **Las soluciones de CipherTrust Database Protection** integran el cifrado de datos en campos sensibles en bases de datos gracias a una gestión de claves segura y centralizada que no requiere modificar aplicaciones de bases de datos. Las soluciones de CipherTrust Database Protection son compatibles con bases de datos de Oracle, Microsoft SQL Server, IBM DB2 y Teradata. • **CipherTrust Manager es el panel de gestión centralizada de la plataforma**. Les permite a las empresas administrar centralizadamente las claves de cifrado, ofrecer controles de acceso granular y configurar las políticas de seguridad. Gestiona las tareas del ciclo de vida de las claves (como generación, rotación, destrucción, importación y exportación), proporciona controles de acceso a claves y políticas basados en funciones, posibilita auditorías e informes robustos y ofrece API REST intuitivas para desarrolladores. Está disponible en factores de forma físicos y virtuales que cumplen con FIPS 140-2 hasta el nivel 3. **Los módulos de seguridad de hardware Luna** generan, almacenan, protegen y administran claves criptográficas que se utilizan para proteger datos confidenciales y aplicaciones críticas. Los HSM Luna ofrecen la mayor cantidad de certificaciones en la industria, incluidos Common Criteria, FIPS 140-2 Nivel 3, ITI, entre otros. Tenga total confianza en su infraestructura, respaldada por una base criptográfica reconocida internacionalmente y certificada por un HSM. Los HSM Luna de Thales brindan una raíz de confianza para las tecnologías existentes y emergentes, incluida la Infraestructura de clave pública (PKI) y las fuertes claves de almacenamiento para la firma de código que mantienen la integridad del código. Thales ofrece también una solución de firma de código personalizada para empresas construidas sobre HSM Luna, contenedores y API REST, disponible on-premises, como un servicio de HSM en la nube y en entornos híbridos. **Protección de datos bajo demanda (DPoD)**es una plataforma basada en la nube que ofrece una amplia gama de servicios de administración de claves y HSM en la nube a través de un sencillo mercado en línea.

Categoría	Requisito	Soluciones de Thales
PROTEGER **Seguridad de los datos (PR.DS)**	PR.DS-2: Los datos en tránsito están protegidos.	**Las soluciones de cifrado de Thales (HSE)** ofrecen la solución certificada y probada ideal para la seguridad de datos en movimiento, incluidas las transmisiones de vídeo y voz urgentes, para empresas y organizaciones gubernamentales: • Los cifradores de red de la serie CN son dispositivos de red de hardware que ofrecen cifrado independiente de la capa de red (Capas 2, 3 y 4) para los datos en tránsito. Estos cifradores de hardware cuentan con certificación para FIPS 140-2 Nivel 3, Common Criteria, NATO y están en DoDIN APL. • La serie CV es un dispositivo virtual reforzado que ofrece un cifrado sólido para datos en movimiento, a través de WAN de portadora de alta velocidad y enlaces SD-WAN, utilizando Network Function Virtualization (NFV).
RESPONDER (RS) **Mitigación (RS-MI)**	RS.MI-3: Las vulnerabilidades identificadas recientemente se mitigan o documentan como riesgos aceptados.	**CipherTrust Intelligent Remediation** integra el descubrimiento de datos confidenciales basado en riesgos con cifrado transparente basado en políticas para mitigar automáticamente el riesgo de exposición de datos. Ayuda a las organizaciones a visualizar los riesgos comerciales y automatizar las acciones de reparación para protegerse contra los ataques de ransomware. **SafeNet Trusted Access** les permite a las organizaciones responder y mitigar el riesgo de ransomware al proporcionar una pista de auditoría inmediata y actualizada de todos los eventos de acceso a todos los sistemas. Los extensos informes automatizados documentan todos los aspectos de la aplicación y autenticación del acceso. Además, el servicio transmite automáticamente los registros a los sistemas SIEM externos.

Un conjunto completo de soluciones para cumplir con el marco de ciberseguridad del NIST

Si bien las soluciones de Thales brindan algunas de las capacidades más importantes en el marco de ciberseguridad del NIST, ninguna empresa por sí sola puede proporcionar un conjunto verdaderamente completo de soluciones para cumplir con los requisitos del NIST. Es por eso que Thales cuenta con más de 400 socios, que se encuentran entre los proveedores de tecnología líderes en el mundo, para brindarles a los clientes un conjunto completo de soluciones e integraciones y cumplir con el marco de ciberseguridad del NIST. Comuníquese con nosotros para saber más sobre cómo podemos ayudarlo a prevenir no solo el ransomware, sino también el malware destructivo, las amenazas internas y otras amenazas persistentes avanzadas.

Acerca de Thales

Thales es un líder mundial en seguridad de datos, en el que los gobiernos y las empresas más reconocidas del mundo confían en ayudarlos a proteger sus datos más confidenciales. Las personas en las que confía para la protección de su privacidad confían en Thales para proteger sus datos. Las empresas se enfrentan a un número cada vez mayor de momentos decisivos relacionados con la seguridad de los datos. Tanto si se trata de elaborar una estrategia de cifrado, como de migrar a la nube o de cumplir los requisitos normativos, puede confiar en Thales para proteger su proceso de transformación digital.