cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Transparent Encryption Protección contra Ransomware

Desafío: el Ransomware bloquea el acceso a datos críticos de la empresa

El ransomware ha ido en aumento desde 2020. Representa e 25% de todas las filtraciones de datos[1]. Los ataques de ransomware pueden detener por completo las operaciones comerciales al bloquear el acceso a datos críticos hasta que se pague un rescate. Se espera que un ransomware ataque a empresas e individuos cada 2 segundos para el año 2031[2].

Las prácticas de seguridad básicas que utilizan controles perimetrales, como firewalls de próxima generación, puertas de enlace seguras para el correo electrónico/web y centrarse en cerrar las brechas de vulnerabilidad por sí solas, no han sido suficientes para prevenir los ataques de ransomware. El principaldesafío que enfrentan las empresas Fortune 500 es proteger los datos críticos para el negocio para que no sean cifrados por procesos y usuarios no autorizados en terminales y servidores.

Solución: Protección contra Ransomware con cifrado transparente CipherTrust

CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) proporciona una forma no intrusiva de proteger archivos/carpetas contra ataques deransomware. CTE-RWP detecta actividad de E/S anormal en archivos que alojan datos críticos para el negocio por proceso.Permite a los administradores alertar/bloquear actividades sospechosas antes de que el ransomware pueda apoderarse de sus puntos finales/servidores.

Ventajas clave

- **Protección de Datos Transparente.** CTE-RWP aplica continuamente la protección contra ransomware por volumen con una configuración mínima y sin modificaciones en ninguna aplicación en el punto final/servidor. Supervisa continuamente la actividad anormal de los archivos causada por procesos infectados con ransomware y alerta/bloquea cuando se detecta dicha actividad.
- **Fácil de implementar.** CTE-RWP permite a los administradores comenzar solo con protección contra ransomware, sin configurar políticas restrictivas de control de acceso y cifrado por archivo/carpeta, que está disponible en una licencia CTE.
- **Detección robusta de ransomware.** CTE-RWP utiliza procesosModelos de aprendizaje automático basados en para detectar dinámicamente actividad de E/S de archivos sospechosos. Identifica y alerta o bloquea ransomware en puntos finales/servidores. Los procesos aprobados se pueden agregar a una lista confiable para evitar el monitoreo.

1 https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

2 https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/#:~:text=Cybersecurity%20Ventures%20predicts%20that%20by,than%20ever%20protecting%20against%20ransomware

Licencia

CTE-RWP tiene licencia por separado. Proporciona un nivel adecuado de detección de ransomware, sin configurar políticas detalladas de control de acceso a nivel de archivo/carpeta en cada punto final/servidor. Combinado con una licencia CTE, los administradores pueden aplicar además un control de acceso y cifrado más detallados. CTE-RWP se puede licenciar por separado o junto con CTE.

Protección de datos adicional contra Ransomware con Cifrado Transparente CipherTrust

Los clientes pueden maximizar la protección contra ransomware en sus terminales/servidores agregando una licencia para CipherTrust Transparent Encryption (CTE), para obtener los siguientes beneficios adicionales que no proporciona CTE-RWP.

Control de acceso detallado

- Define quién (usuario/grupo) tiene derechos para cifrar/descifrar/leer/escribir o enumerar el directorio donde residen los datos críticos para el negocio
- Implementar políticas estrictas de control de acceso en torno a los procesos de copia de seguridad, incluido el cifrado de copias de seguridad para evitar la filtración de datos.
- Lista confiable de archivos (binarios) a nivel de punto de guardia que están aprobados para acceder y cifrar/descifrar carpetas protegidas, incluidas comprobaciones de firmas en aplicaciones confiables para garantizar su integridad.

Cifrado de datos en reposo

- Cifre datos críticos para el negocio, dondequiera que residan en las instalaciones oen las nubes
- Hacer que los datos críticos pierdan valor para los intrusos, ya que no pueden monetizar los datos cifrados amenazando con publicarlos.
- Lista confiable de archivos (binarios) a nivel de punto de guardia que están aprobados para acceder y cifrar/descifrar carpetas protegidas, incluidas comprobaciones de firmas en aplicaciones confiables para garantizar su integridad.

Con MFA para CipherTrust Encryption

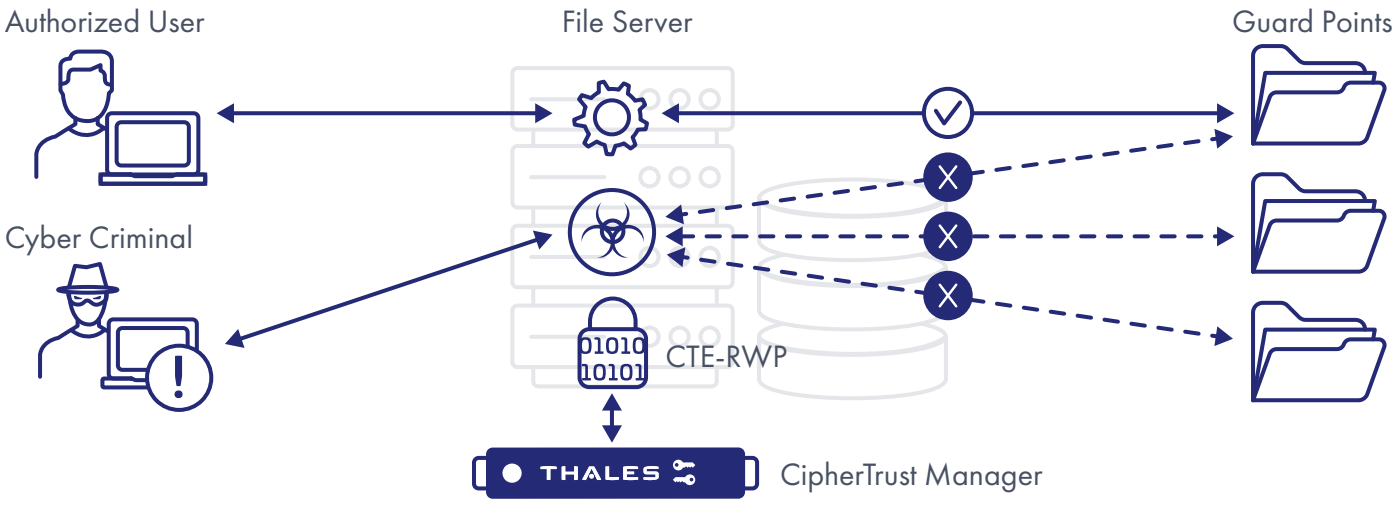
Los clientes pueden agregar autenticación multifactor (MFA) para CipherTrust Encryption (CTE) para obtener una capa adicional de protección a nivel de carpeta/archivo. MFA para CTE solicita a los administradores de sistemas y a los usuarios privilegiados que demuestren un factor adicional de autenticación más allá de las contraseñas cuando intentan acceder a datos confidenciales que se encuentran detrás de los Guard Points.

MFA para CTE está disponible para la plataforma Windows. Admite integraciones con múltiples proveedores de autenticación, incluidos SafeNet Trusted Access de Thales, Okta y Keycloak.

Acerca de Thales

Las personas en las que usted confía para proteger su privacidad confían en Thales para proteger sus datos. Cuando se trata de seguridad de datos, las organizaciones se enfrentan a un número cada vez mayor de momentos decisivos. Ya sea que se trate de crear una estrategia de cifrado, migrar a la nube o cumplir mandatos de cumplimiento, puede confiar en Thales para asegurar su transformación digital.

Tecnología decisiva para momentos decisivos.



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

> cpl.thalesgroup.com <

Contáctenos – Para conocer todas las ubicaciones de las oficinas y la información de contacto, visite cpl.thalesgroup.com/es/contact-us