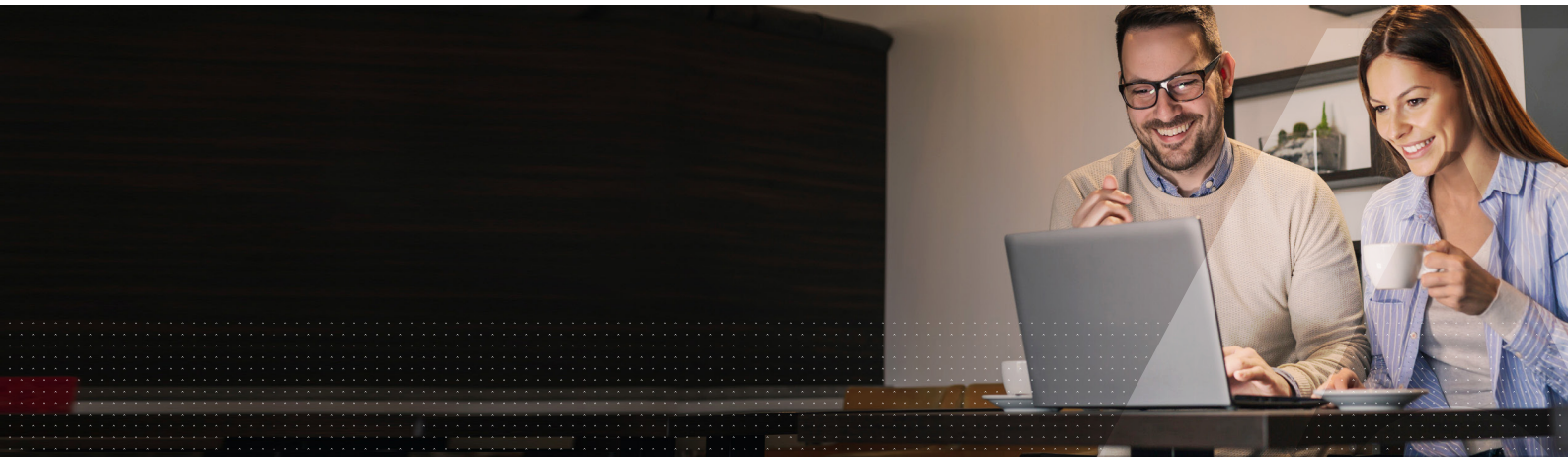
cpl.thalesgroup.com

Google Workspace | THALES
Building a future we can all trust

Soluciones de seguridad de Thales para Google Workspace

Privacidad y confidencialidad mejoradas con cifrado de Google Workspace del lado del cliente y la protección de datos e identidad de Thales



Mejorando la gestión de claves para Google Workspace

Los proveedores de nube y las empresas buscan una seguridad en la nube y un cumplimiento más robustos. Google Workspace aborda este desafío y ahora ofrece opciones mejoradas de privacidad y confidencialidad para Gmail, Google Calendar, llamadas por Google Meet y Google Drive con cifrado del lado del cliente, una solución que permite a los clientes empresariales controlar completamente sus claves de cifrado con CipherTrust Cloud Key Manager y SafeNet Trusted Access, en conjunto o de forma separada.

De esta forma, y adhiriéndose al concepto de «seguridad compartida», Google recomienda que los clientes usen un gestor de claves externo (EKM) y un proveedor de identidad (IDP) para garantizar que solo los individuos autorizados y autenticados puedan acceder a la información protegida. En la actualidad, únicamente Thales ha desarrollado una solución independiente de IDP y gestión de claves.

Cifrado de Google Workspace del lado del cliente con la gestión de claves y protección de identidad de Thales: unidos, mejor

Los clientes que usan cifrado en Google Workspace del lado del cliente pueden disfrutar de un mayor nivel de seguridad y menores gastos de implementación haciendo gala de la solución integrada de principio a fin de Thales, que controla las claves de cifrado de manera separada a los datos confidenciales en la nube, además de proteger las identidades.

Las claves de cifrado del lado del cliente permiten a los proveedores de servicios alojar datos cifrados pero no descifrarlos, garantizando así la privacidad del usuario. Por ejemplo, cuando un usuario accede a su archivo, la clave de cifrado de datos correspondiente se descifra con las claves del cliente únicamente después de que el usuario se haya autenticado mediante autenticación controlada por el cliente.

SafeNet Trusted Access (STA) de Thales, en conjunto con CipherTrust Cloud Key Manager, ofrece a los clientes un IDP independiente y una solución de gestión de claves de parte de un solo proveedor, lo que contribuye a alcanzar sus metas empresariales con una implementación más fluida, una experiencia de usuario superior y un mayor valor.

Thales es un socio multinube de confianza. CipherTrust Cloud Key Manager y STA, usados en conjunto o de manera independiente, permiten a las empresas tanto mantener el control de sus claves de acceso como la seguridad de acceso, a la vez que evitan la dependencia de un proveedor, lo cual es vital para mantener los entornos multinube como parte de iniciativas de transformación digital.

Cómo funciona la solución en conjunto

Un usuario inicia sesión en Google Workspace y se lo redirige a STA para autenticarse y validar su identidad.

- STA autentica al usuario y crea un token de autenticación
- Cuando el usuario crea un archivo de cifrado del lado del cliente, Gmail, Google Calendar o una llamada en Google Meet, el token de autenticación generado por STA y un token de autorización diferente generado por Google se envían a CipherTrust Cloud Key Manager con una clave de cifrado de datos (DEK) generada por Google
- CipherTrust Cloud Key Manager valida el token de autenticación generado por STA con este mismo programa, y valida el token de autorización generado por Google con este último
- Si se validan ambos tokens, CipherTrust Cloud Key Manager cifra la DEK con una clave de cifrado de claves (KEK) generada por CipherTrust y devuelve la DEK cifrada a Google
- En caso de volver a abrir o guardar el archivo, se requerirá validación por parte de CipherTrust Cloud Key Manager, lo que permite que los usuarios autorizados abran la KEK y puedan acceder a la DEK y al archivo

Beneficios fundamentales

Las empresas que pasan cargas de trabajo y aplicaciones a la nube suelen aprovecharse de suites de colaboración, como Google Workspace. Además de ofrecer una amplia gama de beneficios en cuanto a acceder de manera segura y desde cualquier parte y dispositivo, añadir cifrado e identificación externos brinda la capacidad de controlar las claves de cifrado y añade una capa adicional de privacidad y seguridad a los activos empresariales confidenciales que existan en la nube.

Thales es el único proveedor de seguridad que ofrece gestión de claves independiente, IDP, y autenticación, lo que permite a las empresas cumplir con las mejores prácticas de seguridad en la nube para proteger Google Workspace con cifrado del lado del cliente.

La solución integrada de claves y acceso de Thales aporta beneficios tangibles, como:

- **Seguridad:** Permite a las empresas reducir el riesgo de una brecha de datos y de cualquier penalización al poseer sus propios métodos de gestión de claves y seguridad de acceso
- **Implementación fluida:** La integración única de un proveedor con Google Workspace garantiza una implementación rápida y fluida
- **Experiencia superior de usuario:** Los usuarios se pueden beneficiar de un inicio de sesión único en Google Workspace y de sus otros servicios y aplicaciones en la nube

Elementos destacados

Gestión de claves para Google Workspace

CipherTrust Cloud Key Manager ofrece gestión de claves externa y control de políticas para garantizar que los documentos cifrados, Gmail, Google Calendar y las llamadas en Google Meet solo cuentan con el acceso de los usuarios autorizados.

Protección de identidad para el cifrado del lado del cliente

STA actúa como IDP independiente de terceros y autentica a los usuarios que entren en Google Workspace. STA habilita la autenticación del cifrado de Google Workspace del lado del cliente mediante la integración con OIDC.

Mejorando la autenticación y el acceso seguro a Google Workspace

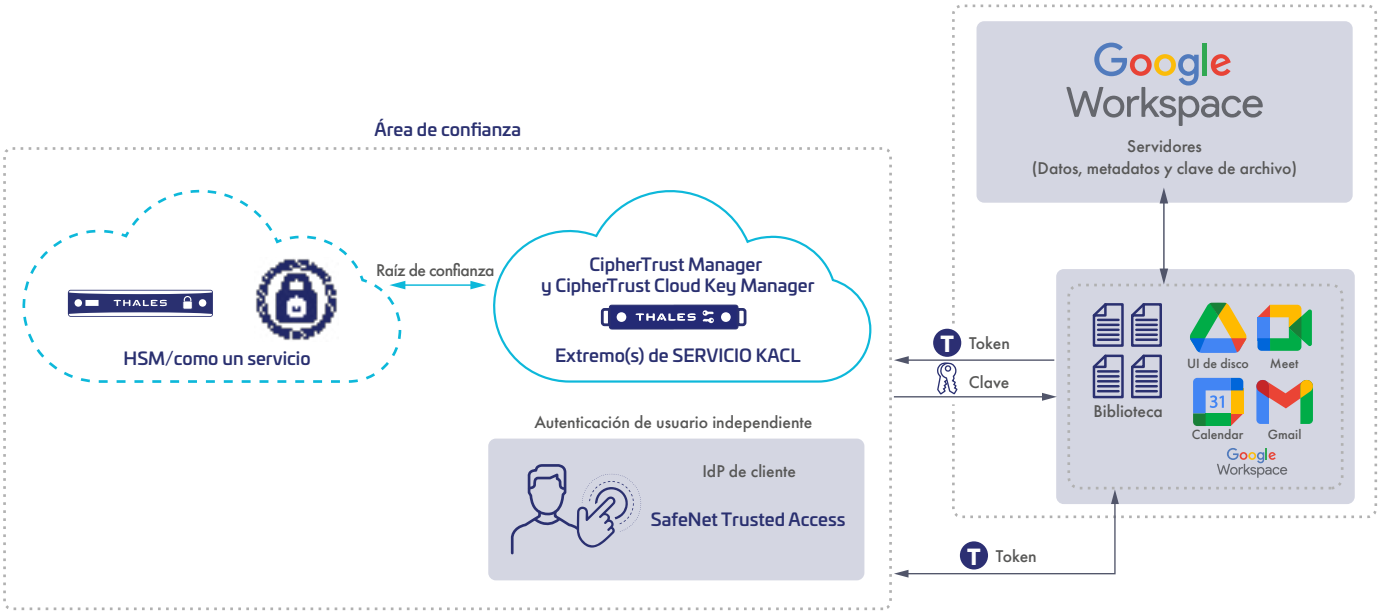
STA se unifica con Google Workspace mediante la integración SAML, lo que permite el inicio de sesión único, y garantiza el nivel apropiado de autenticación cuando los usuarios inician sesión en sus servicios de Google.

Autentificación simple y segura

Implemente un modelo de seguridad Zero Trust mediante conceptos de autenticación primero, acceso después, con una autenticación sólida y continua, un inicio de sesión único y autenticación de múltiples factores en todos los recursos. Entre los métodos de autenticación se incluyen: FIDO, tokens por hardware, tokens de software (aplicaciones de OTP), autenticación push fuera de banda (OOB), autenticación basada en certificados (CBA), autenticación basada en patrones, OOB por mensajes de texto y correos electrónicos, y autenticación contextual.

Comodidad y facilidad

Se puede configurar la reautenticación para usar las credenciales existentes en un periodo de tiempo predeterminado, lo que disminuye la fricción con el usuario sin comprometer la seguridad.



Acerca del cifrado de Google Workspace del lado del cliente

El cifrado de Google Workspace del lado del cliente ayuda a los clientes a reforzar la confidencialidad de sus datos y puede abarcar una amplia gama de requisitos de soberanía de datos y cumplimiento. Los clientes pueden controlar directamente sus claves de cifrado y el servicio de identidad de su elección para acceder a sus claves. Google no puede descifrar los datos del cliente, y los usuarios pueden seguir aprovechándose de la colaboración, acceder al contenido en dispositivos móviles y compartir archivos cifrados de manera externa.

Acerca de Google Workspace

Google Workspace es una plataforma unificada de colaboración y comunicaciones que ofrece a las empresas de cualquier tamaño todo lo que necesitan para conectar, crear y colaborar. Google Workspace incluye aplicaciones como Gmail, Google Meet, Google Calendar, Drive, Docs, Sheets, Slides y más. En workspace.google.com encontrará más información.

Acerca de la gestión de acceso de Thales

Las soluciones de autenticación y gestión de acceso de Thales, líderes en la industria, permiten a las empresas administrar y proteger de manera centralizada el acceso a las aplicaciones basadas en la nube, la web y TI empresarial con un enfoque Zero Trust. Mediante el uso de acceso condicional SSO y métodos de autenticación universal basados en políticas, las empresas pueden prevenir infracciones de forma eficaz, migrar a la nube de forma segura y simplificar el cumplimiento normativo.

Acerca de la protección de datos de Thales

CipherTrust Data Security Platform es una cartera de productos preparada para la nube y diseñada para aliviar muchos de los desafíos a los que se enfrentan los equipos de seguridad a medida que adoptan estrategias multinube. La plataforma ofrece una gama inigualable de soluciones para encargarse tanto de la seguridad de los datos como de la gestión de claves de cifrado. CipherTrust Cloud Key Manager es un componente de la plataforma.

Acerca de Thales

Las personas en las que confía para la protección de su privacidad confían en Thales para proteger sus datos. Cuando se trata de seguridad de datos, las empresas se enfrentan a un número cada vez mayor de momentos decisivos. 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 asegurar su transformación digital.

Tecnología decisiva para momentos decisivos.

> cpl.thalesgroup.com/es <

Póngase en contacto con nosotros – Para conocer la ubicación de las oficinas y nuestros datos de contacto, visite cpl.thalesgroup.com/es/contact-us