



Cisco Spark

Seguridad de Cisco Spark

¿Quién tiene las claves de sus datos de la nube?

¿Su empresa colaboradora accede a su contenido, le retiene o le otorga control?

Aplicaciones de mensajería empresarial típicas: demasiado abiertas

Las aplicaciones de mensajería empresarial típicas ponen en riesgo la seguridad al acceder a su contenido para ofrecer funciones como búsqueda de mensajes, transcodificación de contenido o integración con aplicaciones de terceros.



Aplicaciones de chat para el consumidor: demasiado restrictivas

Las aplicaciones de chat entre consumidores finales suelen estar orientadas hacia la protección de la seguridad del consumidor, ya que ofrecen cifrado de extremo a extremo a costa de la ampliación del sistema y de características que añaden valor.



Cisco Spark: la opción perfecta

Cisco Spark™ reúne lo mejor de estos dos mundos: una plataforma de colaboración en la nube de extremo a extremo y cifrada que aporta a los equipos de TI la capacidad de acceder al contenido y elegir qué permiso, si lo hubiera, proporcionar a Cisco y a terceros.



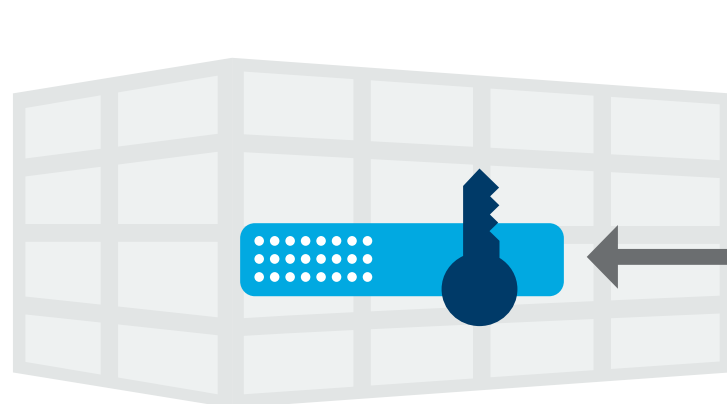
¿Cuál encaja en su modelo de seguridad?



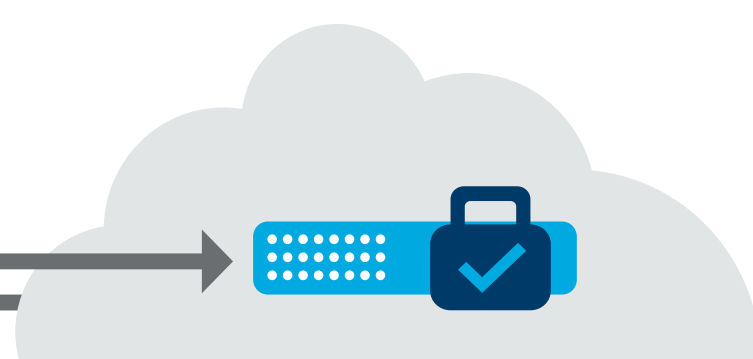
Usted tiene las claves.

Cifrado de extremo a extremo y control sobre el cliente

Cisco Spark hace uso de una arquitectura abierta para la distribución segura de las claves de cifrado, lo que permite a nuestros clientes obtener un control exclusivo de la gestión de sus claves de cifrado y de la confidencialidad de sus datos. Esto significa que el contenido está cifrado para el cliente del usuario y permanece así hasta que llega a su destinatario, sin que ningún intermediario tenga acceso a las claves de descifrado del contenido salvo que la empresa elija explícitamente conceder dicho acceso.



Servidor de claves in situ



Servidor en la nube de almacenamiento de contenido

[Más información >](#)

