Guía de seguridad

Zoom Video Communications, Inc.

Zoom ayuda a empresas y organizaciones a reunir a sus equipos en un entorno fluido para obtener mejores resultados. Nuestra plataforma sencilla y fiable en la nube para vídeo, voz, uso compartido de contenidos y chat se puede ejecutar en todos los dispositivos móviles y de escritorio, en teléfonos y en salas equipadas con sistemas electrónicos.

Para Zoom, la seguridad es la más alta prioridad en las operaciones de su conjunto de productos y servicios. Zoom se esfuerza por ofrecer continuamente un sólido conjunto de características y prácticas de seguridad para satisfacer los requisitos de las empresas en materia de colaboración segura.

El objetivo de este documento es ofrecer información sobre las características y funciones de seguridad disponibles con Zoom. Se supone que el lector de este documento está familiarizado con las funciones de Zoom relacionadas con reuniones, seminarios web, chat, intercambio de archivos y llamadas de voz.

A menos que se indique lo contrario, las funciones de seguridad de este documento se aplican a todo el conjunto de productos de reuniones de Zoom, seminarios web de Zoom, Zoom Rooms y Zoom Voice, en todos los puntos de conexión a través de móviles, tabletas, escritorio, portátiles y sistemas de salas SIP/H.323 compatibles.

Infraestructura

La nube de Zoom es una red mundial exclusiva que se ha creado desde cero para proporcionar experiencias de comunicación de calidad. Zoom funciona en un modo híbrido escalable; los servicios web que proporcionan funciones como la organización de reuniones, la administración de usuarios, las grabaciones de conferencias, las transcripciones de chat y las grabaciones de correo de voz están alojadas en la nube, mientras que los medios de conferencia en tiempo real se procesan en centros de datos de colocación de nivel 1 distribuidos por todo el mundo con certificaciones SSAE 16 SOC 2 tipo 2.

Procesamiento de medios en tiempo real

Una red distribuida de routers de software multimedia de baja latencia conecta la infraestructura de comunicaciones de Zoom. Con estos routers multimedia, todos los datos de la sesión que se originan en el dispositivo del anfitrión y llegan a los dispositivos de los participantes se encaminan dinámicamente entre los puntos de conexión. Las sesiones de Zoom en tiempo real funcionan de forma similar a la conocida operativa móvil de conversación de la red móvil pública.

Compatibilidad con el cortafuegos

Durante la configuración de la sesión, el cliente de Zoom se conecta a través de HTTPS (puerto 443/TLS) a los servidores de Zoom para obtener la información necesaria para conectarse a la reunión o el seminario web correspondiente, y para evaluar el entorno de red actual, como por ejemplo el router multimedia adecuado que se debe utilizar, qué puertos están abiertos y si se utiliza un proxy SSL. Con estos metadatos, el cliente de Zoom determinará el mejor método para la comunicación en tiempo real, intentando establecer conexión automática mediante uso preferente de los puertos UDP y TCP 8801, 8802 y 8804. Para una mayor compatibilidad y soporte de los servidores proxy SSL de la empresa, la conexión también se puede establecer a través de HTTPS (puerto 443/TLS). También se establece una conexión HTTPS para los usuarios que se conectan a una reunión a través del cliente del navegador web de Zoom.

Aplicación de cliente

Seguridad del usuario basada en roles

El anfitrión tiene a su disposición las siguientes funciones de seguridad previas a la reunión:

- Inicio de sesión seguro mediante un nombre de usuario y una contraseña estándar, o inicio de sesión único SAML
- Iniciar una reunión segura con contraseña
- Programar una reunión segura con contraseña

Invitación a una reunión selectiva: El anfitrión puede invitar selectivamente a los participantes por correo electrónico, mensaje directo o SMS. Esto proporciona un mayor control sobre la distribución de la información de acceso a la reunión. El anfitrión también puede crear la reunión para permitir que solo se unan los miembros de un determinado dominio de correo electrónico.

Seguridad de información de la reunión: Zoom conserva la información de los eventos relacionados con una sesión a efectos de facturación y creación de informes. La información del evento se almacena en la base de datos segura de Zoom y está a disposición del administrador de la cuenta del cliente para su revisión en la página del portal del cliente una vez que se haya conectado de forma segura.

Seguridad de la aplicación: Zoom puede cifrar todo el contenido de la presentación en la capa de aplicaciones mediante el algoritmo de 256 bits del Estándar de Cifrado Avanzado (AES).

Controles de política de grupo del cliente de Zoom: se aplica de manera específica al cliente de reuniones de Zoom para Windows y a Zoom Rooms para Windows, pudiendo los administradores definir un amplio conjunto de ajustes de configuración del cliente que se ejecutan a través de los controles de política de grupo de Active Directory.

Cifrado de chat: el cifrado de chat de Zoom permite una comunicación segura en la que solo el destinatario previsto puede leer el mensaje protegido. Zoom utiliza la clave pública y privada para cifrar la sesión de chat con el Estándar de Cifrado Avanzado (AES-256). Las claves de las sesiones se generan con un Id. de hardware exclusivo del dispositivo para evitar que los datos se lean desde otros dispositivos. Esto garantiza que la sesión no se pueda manipular ni escuchar a escondidas.

Seguridad de reuniones

Seguridad del usuario basada en roles

El anfitrión tiene a su disposición las siguientes funciones de seguridad durante la reunión:

- Las reuniones están cifradas de forma predeterminada
- Sala deespera
- Habilitar la espera para que el anfitrión se una
- Expulsar a uno o a todos los participantes
- Finalizar unareunión
- Bloquear unareunión
- Chatear con un participante o con todos los participantes
- Silenciar o reactivar audio de un participante o de todos los participantes
- Colocar marcas de agua al compartir la pantalla
- Firmas deaudio
- Habilitar o deshabilitar la grabación para uno o todos los participantes
- Detener temporalmente la función de compartir pantalla cuando se abre una ventana nueva

Los participantes de la reunión tienen a su disposición las siguientes funciones de seguridad durante la reunión:

- Silenciar/reactivar audio
- Encender/apagar vídeo
- Desenfocar la instantánea en el selector de tareas de iOS

Reunión autentificada por el anfitrión y el cliente: se requiere que el anfitrión se autentique (mediante https) en el sitio de Zoom con sus credenciales de usuario (ID y contraseña) para iniciar una reunión. El proceso de autenticación del cliente utiliza un token exclusivo por cliente y sesión para confirmar la identidad de cada participante que intente unirse a una reunión. Cada sesión tiene un conjunto exclusivo de parámetros de sesión que genera Zoom. Cada participante autenticado debe tener acceso a estos parámetros de sesión junto con el token de sesión exclusivo para poder unirse a la reunión de forma satisfactoria.

Reunión abierta o protegida por contraseña: el anfitrión puede exigir a los participantes que introduzcan una contraseña antes de unirse a la reunión. Esto proporciona un mayor control de acceso y evita que se unan a una reunión invitados no deseados.

Editar o eliminar la reunión: el anfitrión puede editar o eliminar reuniones anteriores o futuras. Esto proporciona un mayor control sobre la disponibilidad de las reuniones.

Acceso a reuniones controlado por el anfitrión: para tener un mayor control de las reuniones, el anfitrión puede exigir a los participantes que solo se unan a la reunión después de que él la haya iniciado. Para mayor flexibilidad, el anfitrión puede permitir que los participantes se unan antes que él. Cuando se unen antes que el anfitrión, los participantes tienen un límite de reunión de 30 minutos.

Seguridad durante la reunión: durante la reunión, Zoom proporciona contenido multimedia en tiempo real y de forma segura a cada uno de los participantes de la reunión de Zoom. Todo el contenido compartido con los participantes en una reunión es solo una representación de los datos originales. Este contenido se codifica y se optimiza para compartirlo mediante una implementación segura, como se indica a continuación:

- Es el único medio posible para unirse a una reunión de Zoom
- Depende completamente de conexiones establecidas sesión por sesión
- Lleva a cabo un proceso exclusivo que codifica todos los datos compartidos
- Puede cifrar todo el contenido de la pantalla compartida usando el estándar de cifrado AES 256
- Puede cifrar la conexión de red a Zoom mediante el estándar de cifrado TLS de 256 bits
- Proporciona una identificación visual de cada participante de la reunión

Acceso a reuniones controlado por el anfitrión

Entre los métodos de autenticación se incluye el inicio de sesión único (SSO) con SAML u OAuth.

Con el SSO, el usuario se conecta una vez y obtiene acceso a varias aplicaciones sin que se le pida que se conecte de nuevo en cada una de ellas. Zoom admite SAML 2.0, que permite la autenticación y autorización basada en web, incluido el SSO. SAML 2.0 es un protocolo XML que utiliza tokens de seguridad que contienen afirmaciones para transferir información sobre un usuario entre una autoridad SAML (un proveedor de identidad) y un servicio web (como Zoom). Zoom trabaja con Exchange ADFS 2.0 y con otras plataformas de gestión de identidad empresarial, entre ellas, Centrify, Fugen, Gluu, Okta, OneLogin, PingOne, Shibboleth, Symplified y muchas más. Zoom puede asignar atributos para aprovisionar un usuario a un grupo diferente con controles de funciones.

El aprovisionamiento basado en OAuth funciona con Google o Facebook OAuth para un aprovisionamiento instantáneo. Zoom también ofrece una llamada API para aprovisionar previamente usuarios de cualquier servidor de base de datos.

Asimismo, su organización o universidad puede añadir usuarios a su cuenta de forma automática con dominios administrados. Una vez que se apruebe la solicitud de dominio administrado, se añadirán a su cuenta todos los usuarios, nuevos y existentes, que tengan su dominio de dirección de correo electrónico.

Controles administrativos

La cuenta del administrador tiene a su disposición las siguientes funciones de seguridad:

- Opciones de inicio de sesión seguro mediante un nombre de usuario y una contraseña estándar o SSO SAML
- Incorporación de usuario y administrador a la cuenta
- Subir o bajar el nivel de suscripción de los usuarios

- Eliminar el usuario de la cuenta
- Revisar la facturación y los informes
- Administrar el panel de control de cuentas y las grabaciones en la nube

API de características/opciones especiales de seguridad

Hay disponibles API para integrar Zoom con aplicaciones del cliente personalizadas y aplicaciones de terceros. Cada cuenta de cliente puede incluir credenciales de clave de integración de API gestionadas por el administrador de la cuenta de cliente. Las llamadas a la API se transmiten de forma segura a través de servicios web seguros y es necesario autenticar la API.

Conector de reunión

El conector de reunión de Zoom es un método híbrido de implementación en la nube, que permite a un cliente implementar un router multimedia de Zoom (software) dentro de la red interna del cliente.

Los metadatos de usuarios y reuniones se gestionan en la infraestructura de comunicaciones de Zoom, pero la reunión se aloja en la red interna del cliente. Todo el tráfico de la reunión en tiempo real, incluidos audio, vídeo e intercambio de datos, pasa por la red interna de la empresa. De este modo se aprovecha la configuración de seguridad de red existente para proteger el tráfico de la reunión.

Cuando los clientes eligen un despliegue híbrido, tienen la posibilidad de segmentar por tipo de usuario, donde los tipos Pro y gratuito (Básico) utilizarán la nube y los tipos Business y Enterprise utilizarán la solución in-situ.

Si el sistema in-situ está fuera de línea, la reunión se revertirá automáticamente a la nube. Tanto nuestras soluciones en la nube como in-situ están diseñadas con mecanismos de tolerancia a errores y de equilibrio de carga al implementarse.

Zoom Rooms

Zoom Rooms es un sistema de sala de conferencias basado en el software de Zoom. Ofrece conferencias de audio y vídeo, uso inalámbrico compartido de contenidos y calendario integrado que se ejecuta en hardware estándar. Para establecer las comunicaciones se utiliza el cifrado TLS de 256 bits y se aplica el cifrado AES-256 a todo el contenido compartido. La aplicación Zoom Rooms está protegida con Código de Bloqueo de la Aplicación. El Código de Bloqueo de la Aplicación para Zoom Rooms es un código de bloqueo numérico de 1-16 dígitos que se utiliza para proteger la aplicación de Zoom Rooms. Así se evitan cambios no autorizados en la aplicación de Zoom Rooms y en la configuración del hardware utilizado con la misma.

Chat de Zoom

El chat continuo multiplataforma es una característica de las reuniones de Zoom que permite a los usuarios comunicarse por chat y compartir archivos de forma individual o en grupos. Los usuarios pueden hacer clic en "Reunión" desde cualquier chat para iniciar una reunión con vídeo de Zoom de forma instantánea con los participantes del grupo. El chat se puede cifrar para configuraciones compatibles con la Ley estadounidense de transferencia y responsabilidad de seguro médico (HIPAA).

Zoom Phone

Zoom Phone es un sistema de telefonía en la nube disponible como complemento de la plataforma de Zoom. La compatibilidad con llamadas entrantes y salientes a través de la red telefónica pública conmutada (PSTN) y las funciones de telefonía perfectamente integradas permiten a los clientes sustituir su solución PBX existente y consolidar todos sus requisitos de comunicación y colaboración empresarial en su plataforma de vídeo favorita.

Mediante el protocolo de voz sobre IP (VoIP) basado en estándares para ofrecer los mejores servicios de voz de su clase, Zoom Phone ofrece una alternativa segura y fiable a las soluciones PBX tradicionales in situ. La configuración de la llamada y las funciones durante la llamada se ofrecen a través del protocolo de inicio de sesión (SIP). Con el soporte de OPUS como códec preferente para garantizar la mayor calidad posible, Zoom Phone también admite códecs adicionales estándar del sector G.722, G.711 y G.729 para la transcodificación de medios.

Autenticación

- El registro SIP de Zoom Phone se autentica mediante cifrado AES de 128 bits TLS 1.2

Cifrado de medios

- Los medios de VoIP se transportan y protegen mediante Protocolo Seguro de Transporte en Tiempo Real (SRTP) con cifrado AES-128

Emparejamiento de red privada

- Zoom ha establecido enlaces de emparejamiento directo de red privada entre los centros de datos de Zoom Phone y las redes de proveedores de servicios PSTN de Zoom Phone para garantizar la máxima protección.

Llamadas de emergencia

- Zoom Phone es compatible con los servicios de emergencia mejorados E911 (EE.UU./CAN) para proporcionar la ubicación de la persona que llama al punto de respuesta de seguridad pública (PSAP) local según lo exige la ley. Las direcciones de localización de llamadas de origen se pueden definir y asignar en el nivel de cuenta y de usuario individual.
- Las llamadas de emergencia realizadas desde la aplicación móvil de Zoom en smartphones iOS y Android se transmitirán automáticamente de forma predeterminada a la función de llamadas de red móvil salientes nativas del dispositivo móvil y sortearán el servicio de Zoom Phone para redirigir la llamada de emergencia directamente al PSAP del operador de la red móvil.
- Si lo desean, los administradores de Zoom Phone pueden interceptar y redirigir automáticamente las llamadas de emergencia a equipos de respuesta internos.

Fraude de tarifas telefónicas

- Zoom Phone impide el fraude de tarifas telefónicas mediante el control de acceso y las capacidades de detección automatizada. Nuestro departamento de seguridad supervisa activamente las cuentas de los clientes para detectar patrones de llamadas irregulares y notificará a los clientes de posibles actividades fraudulentas.

Listas negras de llamadas

- Las listas negras personales y globales personalizables permiten a usuarios y administradores añadir y gestionar fácilmente números de teléfono bloqueados.

Invocación de la función Elevar a reunión

- Cuando se eleva una llamada de Zoom Phone a una reunión de Zoom, todas las funciones de seguridad de la reunión de Zoom disponibles se aplicarán a esta interacción.

Seminarios web de Zoom

En los seminarios web con vídeo de Zoom, hasta 100 ponentes pueden llevar a cabo presentaciones con vídeo, audio y función de compartir pantallas con hasta 10 000 participantes de solo visualización. Estos seminarios web ofrecen opciones de inscripción, informes, preguntas y respuestas, votaciones, función de levantar la mano para intervenir, indicadores de atención y grabación en formato MP4/M4A. Los seminarios web con vídeo de Zoom se pueden transmitir por YouTube y Facebook Live para llegar a una audiencia en vivo ilimitada. Los ponentes son plenos participantes de la reunión. Pueden ver y enviar vídeo, compartir pantalla, realizar anotaciones, etc. Las invitaciones a los ponentes se envían por separado de las de los asistentes al seminario web. Los contenidos de los seminarios web y el uso compartido de pantalla están protegidos mediante AES 256 y se comunican a través de una red segura que utiliza el estándar de cifrado de 256 bits.

Registro en el seminario web

- Aprobar registro manualmente: el anfitrión del seminario web aprobará o rechazará manualmente si un usuario inscrito recibe la información para unirse al seminario web.
- Aprobar a los inscritos automáticamente: todos los inscritos en el seminario web recibirán automáticamente información sobre cómo unirse al seminario web.

Seminario web sin registro

- Una sola vez: los asistentes se unirán al seminario web solo una vez. Después de que el seminario web termine, los asistentes no podrán usar la misma información para unirse al seminario web.
- Recurrente: los asistentes podrán unirse repetidamente al mismo seminario web con la información aportada.

Almacenamiento de grabaciones

Zoom ofrece a los clientes la posibilidad de grabar y compartir sus reuniones, seminarios web y llamadas de Zoom Phone. Las grabaciones de las reuniones y seminarios web se pueden almacenar en el dispositivo local del anfitrión con la opción de grabación local o bien, las reuniones, seminarios web y llamadas de Zoom Phone se pueden almacenar en la nube de Zoom con la opción de Grabación en la nube (disponible para clientes de pago). Las grabaciones que se almacenan de forma local en el dispositivo del anfitrión se pueden cifrar, si lo desea, usando varias herramientas gratuitas o disponibles a nivel comercial.

Las Grabaciones en la nube se procesan y almacenan en la nube de Zoom una vez que termina la reunión. Se pueden proteger con contraseña o poner a disposición de los espectadores que han iniciado sesión con el correo electrónico de un dominio concreto. Las grabaciones se almacenan en formato de audio y vídeo o solo de audio. Los mensajes de chat durante las reuniones, los archivos compartidos y las transcripciones de las reuniones se pueden guardar de manera opcional en la nube de Zoom, donde también se almacenan cifrados. El anfitrión de la reunión puede gestionar sus grabaciones a través de la interfaz web protegida. Las grabaciones se pueden descargar, compartir o eliminar. Las grabaciones del correo de voz de Zoom Phone se procesan y se almacenan en la nube de Zoom, y se pueden administrar a través del cliente de Zoom protegido.

Recuento de personas en Zoom Rooms

El recuento de personas de Zoom Rooms es una función que está desactivada de forma predeterminada, pero que pueden activar los administradores de la sala. Esta función permite a los administradores ver datos sobre el número de participantes en las reuniones de la sala que se han unido desde Zoom Rooms.

Esta función opera capturando imágenes a lo largo de la reunión. Las imágenes se almacenan temporalmente en el disco duro local de Zoom Rooms y nunca se envían a la nube. Una vez que termina la reunión, las imágenes almacenadas a nivel local se utilizan para contar el número máximo de participantes visibles en las reuniones de la sala. A lo largo de este proceso, la detección de rostros (sin vínculos con información personal) se utiliza para contar a las personas en función de las imágenes capturadas. Una vez que las imágenes se han procesado para captar el número de personas, estas se borran permanentemente.

Al habilitar la función de recuento de participantes para Zoom Rooms, usted reconoce su obligación de cumplir todas las leyes y que es su responsabilidad asegurarse de notificar adecuadamente a los usuarios que esta función está habilitada, así como de haber obtenido el consentimiento oportuno de los interesados en cumplimiento de las normas de registro o privacidad aplicables tanto para la recopilación como para el almacenamiento de estos datos.

Privacidad

Zoom almacena únicamente información básica en la información del perfil de la cuenta de usuario:

- Dirección de correo electrónico
- Contraseña de usuario (con sal, con hash)
- Nombre
- Apellido(s)
- Nombre de la compañía (opcional)
- Número de teléfono de la compañía (opcional)
- Imagen de perfil (opcional)

Para obtener más información acerca de nuestra política de privacidad, visite https://zoom.us/es-es/privacy.html.

Detalles de facturación

Zoom utiliza un socio externo que cumple con PCI para procesar el pago y gestionar todos los aspectos de facturación. No almacenamos en nuestra base de datos información de tarjetas de crédito de los usuarios ni información de facturación.

Certificaciones de seguridad y privacidad

SOC2:

El informe SOC 2 ofrece garantía de terceros de que el diseño de Zoom y nuestros procesos y controles internos cumplen los estrictos requisitos de auditoría establecidos por las normas del Instituto estadounidense de contadores públicos certificados (AICPA) en materia de seguridad, disponibilidad, confidencialidad y privacidad. El informe SOC 2 es el estándar de garantía de facto para proveedores de servicios en la nube.

TRUSTe:

TRUSTe ha certificado las prácticas y declaración de privacidad de Zoom y también actuará como proveedor de resolución de conflictos para las reclamaciones relacionadas con privacidad. Zoom se compromete a respetar su privacidad. Si tiene alguna duda no resuelta acerca de la privacidad o del uso de los datos que no hayamos abordado satisfactoriamente, póngase en contacto con nuestro proveedor de resolución de conflictos de terceros con sede en los EE. UU. (sin coste alguno) en https://feedback-form.truste.com/watchdog/request.

Escudo de privacidad UE-EE. UU.:

Zoom participa en el Marco del Escudo de Privacidad UE-EE. UU. y ha certificado su cumplimiento del mismo. Zoom se ha comprometido a someter todos los datos personales recibidos de los países miembros de la Unión Europea (UE), en base al Marco del Escudo de Privacidad, a los principios correspondientes del mismo. Para obtener más información acerca del Marco del Escudo de Privacidad UE-EE. UU., visite la lista del Escudo de Privacidad del Departamento de Comercio de los EE. UU.https://www.privacyshield.gov/list.

FedRAMP:

Zoom tiene autorización para operar bajo el Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) de los EE. UU., un programa de todo el gobierno que proporciona un modelo estandarizado para la evaluación de la seguridad, la autorización y la supervisión continua de los productos y servicios en la nube utilizados por las agencias federales.

Empresas, organizaciones sanitarias e instituciones educativas de todo el mundo utilizan la plataforma Zoom a diario para establecer conexión con sus equipos, hacer crecer sus organizaciones y cambiar el mundo. Para Zoom, la privacidad y la seguridad son la mayor prioridad en las operaciones del ciclo de vida de nuestra infraestructura de comunicaciones y redes de conexión de reuniones. Además, nos esforzamos por aportar continuamente un sólido conjunto de funciones de seguridad para lograr nuestro objetivo de proporcionar las comunicaciones unificadas centradas en la tecnología de vídeo más eficientes y seguras.