CloudConnexa / Ficha técnica - Abril 2025

CloudConnexa®

El servicio de red segura en la nube que ofrece acceso a la red de confianza cero (ZTNA) y funciones esenciales de seguridad (SSE).

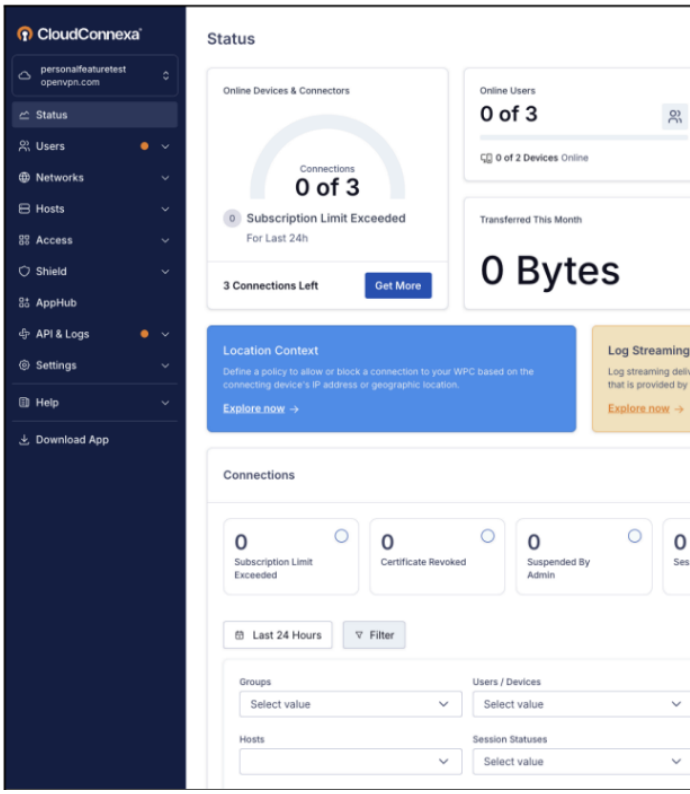
CloudConnexa permite a su personal remoto, híbrido o presencial trabajar de forma segura desde cualquier lugar, lo que proporciona a su empresa una mayor flexibilidad sin riesgo agregado.

CloudConnexa permite establecer un acceso remoto seguro a sus redes privadas y recursos críticos, aplicando de forma continua el modelo de confianza cero (Zero Trust). Esto impide el movimiento lateral dentro de la red y garantiza que solo dispositivos y ubicaciones verificadas puedan establecer conexión.

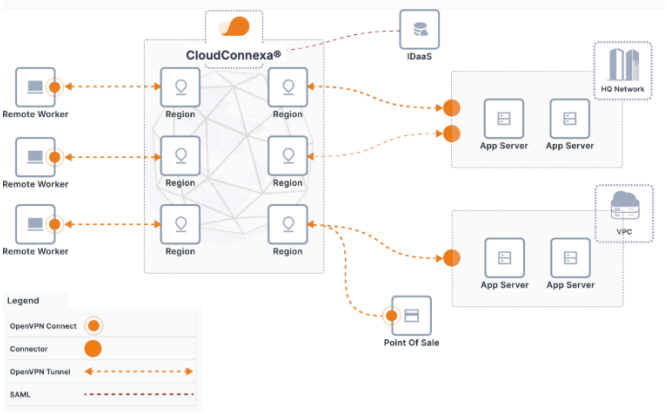
Para reforzar la protección de sus datos confidenciales, CloudConnexa permite convertir sus herramientas SaaS en aplicaciones privadas, accesibles únicamente a través de su entorno seguro. Esto reduce significativamente la superficie de ataque y neutraliza el riesgo asociado a credenciales comprometidas.

Además, incorpora filtrado IDS/IPS y de contenidos, bloqueando ciberamenazas comunes y evitando el acceso a contenido no deseado. Así, sus usuarios pueden navegar con seguridad y sin distracciones.

A diferencia de otras soluciones, CloudConnexa elimina el costo y la complejidad de implementar redes seguras, al ofrecerlas como un servicio con una gestión simple e intuitiva. Con funciones integradas de seguridad avanzada y acceso Zero Trust (ZTNA), CloudConnexa es una solución todo en uno que permite a su empresa operar de forma segura, ágil y eficiente, sin necesidad de infraestructura compleja ni configuraciones técnicas extensas.



¿Cómo funciona CloudConnexa?



Al suscribirse a CloudConnexa, se crea automáticamente una nube privada virtual de amplio alcance (WPC), diseñada exclusivamente para su organización. Esta red privada se extiende por más de 30 puntos de presencia (PoP) distribuidos estratégicamente en todo el mundo.

Todos los PoP están interconectados mediante una topología de malla completa, lo que garantiza rutas directas y alternativas entre cualquier par de puntos, asegurando así alto rendimiento y redundancia.

Puede conectar sus aplicaciones y redes a esta infraestructura mediante IPsec o el protocolo OpenVPN, utilizando el software OpenVPN Connector en sus servidores de aplicaciones, máquinas virtuales o routers compatibles.
Una vez configurada la red, los empleados de su organización pueden acceder de forma segura a estas aplicaciones instalando la app OpenVPN Connect en sus dispositivos y conectándose al PoP más cercano, asegurando una experiencia rápida, segura y confiable.

Características	¿Qué es?
Administración simple	
Portal web de administración	Una interfaz fácil de usar para gestionar sus redes, dispositivos, controles de acceso y más.
Asistentes de configuración	Configuraciones con clics para redes, hosts, IDS/IPS y filtrado de contenido.
Compartición de aplicaciones (AppHub)	Una extranet segura para compartir aplicaciones privadas con otras empresas y departamentos dentro de su organización.
Compatibilidad con clientes OpenVPN Connect (SO)	Los clientes OpenVPN Connect están disponibles para Android, iOS, Windows y macOS.
Conectividad	
Compatibilidad con IPv4 e IPv6	Soporta el creciente número de dispositivos IoT y redes de su organización sin necesidad de dispositivos dual-stack o soluciones alternativas.
Data Channel Offload (DCO)	Aumenta la velocidad y el rendimiento de sus conexiones VPN al trasladar la encriptación y desencriptación al espacio del núcleo (kernel).
Compatibilidad con protocolos OpenVPN e IPsec	Conecta redes a los PoP de CloudConnexa usando OpenVPN o IPsec, ambos con amplio soporte en equipos de red.
Presencia global (más de 30 PoPs en todo el mundo)	Forma una red troncal de alta capacidad con PoPs distribuidos en 6 continentes, compuesta por servidores de alto rendimiento y multi-tenant.
Topología de malla completa (Full-Mesh)	Habilita múltiples rutas de conexión y rutas directas entre más de 30 PoPs a nivel mundial para mayor redundancia y menor latencia de tráfico.
Compatibilidad total con aplicaciones (TCP, UDP, IP)	Soporta cualquier aplicación que utilice TCP y UDP, asegurando que CloudConnexa pueda gestionar y proteger todo el tráfico de red necesario para su empresa.

Características	¿Qué es?
Autenticación	
Soporte para LDAP y SAML	Centraliza la gestión de usuarios y proporciona acceso seguro y fácil mediante inicio de sesión único (SSO), reduciendo la necesidad de múltiples credenciales y mejorando la experiencia del usuario.
Soporte para SCIM	Optimiza el aprovisionamiento y desaprovisionamiento de usuarios y reduce la carga administrativa al automatizar el intercambio de identidades de usuario entre CloudConnexa y tu proveedor de identidad (IdP).
Autenticación multifactor (MFA)	Añade una capa adicional de seguridad mediante MFA vía correo electrónico o una app de autenticación (por ejemplo, Google Authenticator).
Seguridad integrada	
Bloqueo de perfil del dispositivo (Verificación de identidad del dispositivo)	Evita la transferencia del perfil OpenVPN (que contiene un certificado digital) de un dispositivo autorizado para reducir la superficie de ataque.
Políticas de postura del dispositivo	Asegura que los dispositivos cumplan con reglas predefinidas para conectarse y mantenerse conectados a tu WPC, lo cual puede incluir la versión del sistema operativo, software antivirus, comprobaciones de cifrado de disco, entre otros.
Políticas de contexto de ubicación	Permite o bloquea conexiones basadas en si la dirección IP del dispositivo coincide con un rango específico o país (geolocalización por IP).
IDS/IPS integrado (Cyber Shield)	Supervisa y bloquea automáticamente el tráfico malicioso por categoría o nivel de amenaza para mejorar la seguridad de tu red.
Filtro de contenido y web (Cyber Shield)	Bloquea la resolución de dominios de sitios web que pertenezcan a una de las 43 categorías no deseadas o inseguras (también puedes personalizar acciones para dominios específicos con listas de permitidos y bloqueados).
Grupos de acceso	Define qué grupos de usuarios y redes tienen acceso a qué recursos, incluyendo otros hosts y redes junto con sus aplicaciones y servicios IP, para aplicar controles de acceso.
Enrutamiento Avanzado	
Enrutamiento basado en dominios de aplicaciones	Simplifica el enrutamiento de red utilizando nombres de dominio en lugar de subredes IP para resolver conflictos de IP y permite definir fácilmente recursos y configurar el acceso a ellos.
Conectar redes con direcciones IP superpuestas	Diferencia redes y sus direcciones IP mediante nombres de dominio totalmente calificados (FQDN), permitiendo que el tráfico llegue al destino correcto a pesar del solapamiento de IPs.
Enrutamiento inteligente	Optimiza la ruta hacia el destino según la proximidad geográfica y las características de la red.
Acceso a Internet restringido	Bloquea el acceso a Internet —excepto a destinos de confianza o privados— para grupos de usuarios y redes seleccionados, protegiendo contra amenazas.
Visibilidad Accionable	
Visibilidad de acceso	Garantiza que se apliquen los controles de acceso deseados y elimina puntos ciegos de seguridad causados por aplicaciones no detectadas, mostrando qué recursos privados se acceden y por quién.
Registro DNS	Captura todas las solicitudes de resolución DNS para mostrar los dominios y subdominios visitados, e indica si las solicitudes fueron exitosas, bloqueadas o fallidas (incluye quién hizo la solicitud, el registro DNS y más, para mejorar políticas de seguridad y resolver problemas de conectividad).

Características	¿Qué es?
Automatización y Registros	
Transmisión de registros (Log Streaming)	Almacena datos y eventos recopilados de Visibilidad de Acceso, Estado de Conexión, Cyber Shield y Registro de Auditoría en un bucket de AWS S3 para enviarlos a tu solución SIEM para su procesamiento.
Registro de auditoría (Audit Log)	Permite llegar al origen de todas las modificaciones realizadas en tu WPC para facilitar la solución de problemas y auditorías, con visibilidad sobre qué cambió, quién lo hizo y cuándo.
API de CloudConnexa	Se integra con otros sistemas para gestionar tu WPC de forma programática, automatizar flujos de trabajo y mucho más.
IaC usando Terraform	Automatiza tu configuración de CloudConnexa, gestión de usuarios, control de acceso y más, mediante código para asegurar consistencia y facilitar la escalabilidad.

Escucha lo que dicen nuestros clientes

"El equipo de implementación de CloudConnexa fue excepcional. Me guiaron con precisión en la configuración de túneles VPN IPsec utilizando gateways Unifi. Desde entonces, el sistema ha funcionado de forma impecable, proporcionando una conectividad confiable entre nubes a través de SD-WAN."

— Administrador de Sistemas, Greypool

"El proceso de instalación de OpenVPN es sencillo y seguro. Una vez cargado, puedo conectarme a los sistemas de mis clientes siempre que necesitan ayuda. Su portal es claro y fácil de usar, y el soporte al cliente es rápido y eficiente."

— Sam C., Director de Pequeña Empresa

"Lo que más valoro es que cada vez que se activa la VPN, el usuario debe autenticarse mediante inicio de sesión único (SSO). Esto nos permite vincular todos nuestros sistemas críticos a la VPN y, en caso necesario, revocar fácilmente el acceso desactivando la cuenta principal del usuario a través del SSO."

— Chays V., Jefe de Operaciones, Pequeña Empresa

Vea lo que otros dicen sobre CloudConnexa