CloudConnexa / Datasheet – April 2025

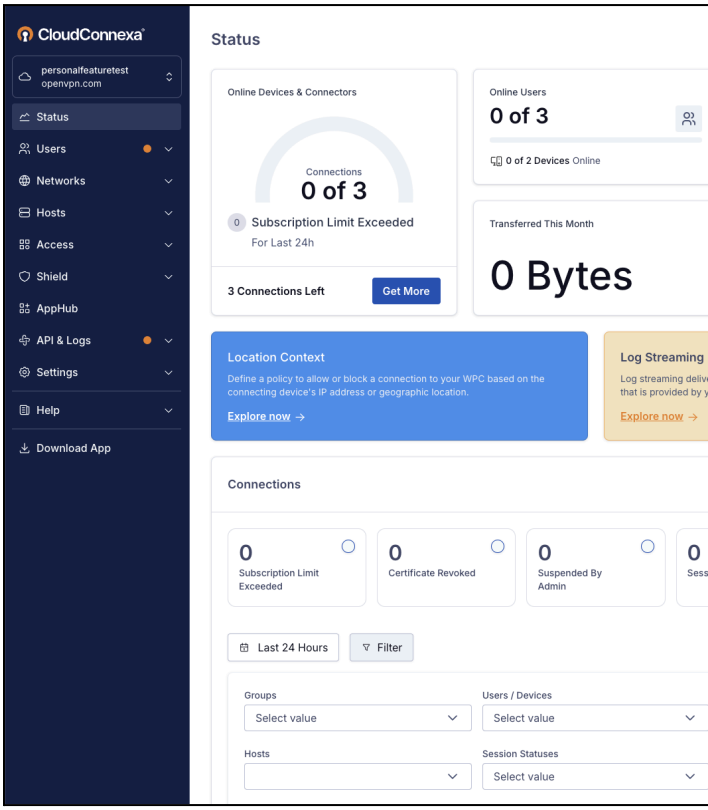
# CloudConnexa®

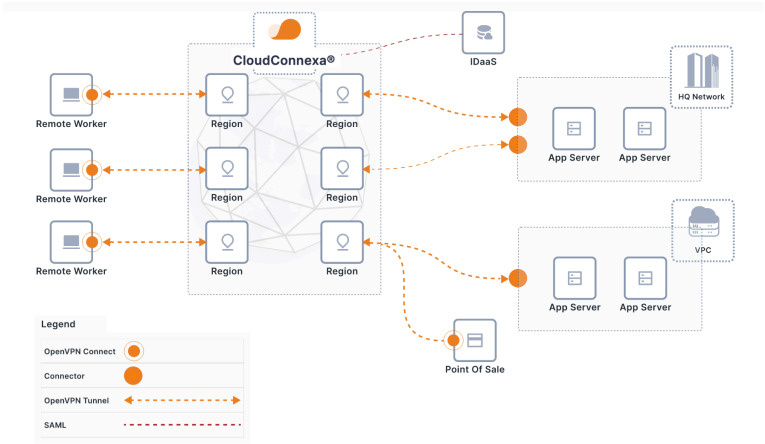
The cloud-delivered secure networking service that delivers zero trust network access (ZTNA) and essential security service edge (SSE) capabilities.

CloudConnexa lets your remote, hybrid, or in-person workforce securely work from anywhere, giving your business greater flexibility without added risk.

You can provide secure remote access to your private networks and resources with continuous zero-trust enforcement, preventing lateral movement and ensuring that connections come from trusted devices and locations. To strengthen the security of your sensitive data, CloudConnexa also lets you turn your essential SaaS tools into private applications, making them accessible only from CloudConnexa. This effectively reduces your attack surface and renders stolen or leaked credentials useless. Plus, CloudConnexa's built-in IDS/IPS and content filtering make it easy to block common cyber threats and undesirable content so your users can confidently browse the web free of distractions.

Unlike other solutions, CloudConnexa takes the cost and complexity out of secure networking by providing it as a service with intuitive management. With built-in security and ZTNA features, CloudConnexa is the all-in-one security and networking solution that lets your business operate safely and efficiently.




## How does CloudConnexa work?

When you sign up for CloudConnexa, a virtually dedicated worldwide private network – Wide-area Private Cloud (WPC) – is created exclusively for your use, encompassing more than 30 worldwide points of presence (PoP). All the PoPs are connected in a full-mesh topology, providing direct and alternate routes between any two PoPs for high performance and redundancy. You can easily connect your applications and networks to these PoPs using IPsec or OpenVPN, by running OpenVPN Connector software on your application servers or lightweight virtual machines on your networks, or by using OpenVPN protocol compatible routers. Your organization's workforce can then access these applications by installing the OpenVPN Connect app on their devices and connecting to the closest PoP.

| Features | What is it? |
|---|---|
| **Simple Administration** | |
| Administration web portal | A user-friendly interface for managing your networks, devices, access controls, and more |
| Configuration wizards | Point-and click configurations for networks, hosts, IDS/IPS, and content filtering |
| Application sharing (AppHub) | A secure extranet for sharing private applications with other businesses and departments within your organization, giving them access to necessary data or services |
| OpenVPN Connect client OS support | OpenVPN Connect clients are available for Android, iOS, Windows, and macOS |
| **Connectivity** | |
| IPv4 and IPv6 support | Supports your organization's growing number of IoT devices and networks without dual-stack devices or workarounds |
| Data Channel Offload (DCO) | Increases the speed and performance of your VPN connections by relocating data channel encryption and decryption to the kernel space |
| OpenVPN and IPsec protocol support | Connects networks to CloudConnexa PoPs using OpenVPN or IPsec–both with broad support across networking equipment |
| Global presence (30+ PoPs worldwide) | Forms a high-bandwidth core network of PoPs — each with a group of high-performance, multi-tenant servers — spread across 6 continents |
| Full-Mesh topology | Unlocks multiple connection paths and direct routes across 30+ worldwide PoPs to reach your sites and devices for increased redundancy and reduced traffic latency |
| Full application support TCP, UDP, IP | Supports any application that communicates using TCP and UDP, ensuring CloudConnexa can manage and secure all network traffic for the services your organization depends on |

| Features | What is it? |
|---|---|
| **Authentication** | |
| LDAP and SAML support | Centralizes user management and provides secure, easy access through Single Sign-On (SSO), reducing the need for multiple credentials and improving the user experience |
| SCIM support | Streamlines user provisioning and deprovisioning and reduces administrative overhead by automating the exchange of user identities between CloudConnexa and your IdP |
| Multi-factor authentication | Adds an extra layer of security with MFA via email or an authenticator app (e.g. Google Authenticator) |
| **Built-in Security** | |
| Device profile lock (Device Identity Verification Enforcement) | Prevents the transfer of an authorized device's OpenVPN profile (that contains a digital certificate) to reduce your attack surface |
| Device Posture policies | Ensures devices meet predefined rules to connect and stay connected to your WPC, which can include OS version, antivirus software and disk encryption checks, and more |
| Location Context policies | Allow or block connections based on whether a device's IP address matches a specific range or a country (IP address geolocation) |
| Built-in IDS/IPS (Cyber Shield) | Automatically monitors and blocks malicious traffic by category or threat priority to enhance your network security |
| Content and web filtering (Cyber Shield) | Blocks domain name resolutions for websites that fall into one of 43 undesirable or unsafe categories (You can also customize actions for specific domains with allow and block lists.) |
| Access Groups | Define which user groups and networks have access to what, including other hosts and networks along with their applications and IP services, to enforce your access controls |
| **Advanced Routing** | |
| Application Domain-based Routing | Simplifies network routing using domain names instead of IP address subnets to resolve IP overlap, and allows you to easily define resources and configure access to them |
| Connect networks with overlapping IP addresses | Differentiate networks and their IP addresses with unique Fully Qualified Domain Names (FQDNs), allowing traffic to reach the correct destination despite there being IP overlap |
| Smart routing | Optimizes the route to the destination based on geographic proximity and network characteristics |
| Restricted internet access | Blocks internet access — except to trusted internet and private destinations — for select user groups and networks to shield users against threats |
| **Actionable Visibility** | |
| Access Visibility | Ensures desired access controls are enforced and eliminates security blindspots posed by undiscovered apps with visibility into which private resources get accessed and by whom |
| DNS Log | Captures all DNS resolution requests made to show the domains and subdomains visited and whether requests were successful, blocked, or failed (See who made the request, the DNS record, and more to improve security policies and troubleshoot connectivity issues.) |

| Features | What is it? |
|---|---|
| **Automation & Logs** | |
| Log Streaming | Stores data and events gathered from Access Visibility, Connection Status, Cyber Shield, and Audit Log into an AWS S3 bucket to route to your SIEM solution for processing |
| Audit Log | Get to the root of all modifications made to your WPC for quicker troubleshoots and audits with visibility into what exactly changed, who did it, and when it happened |
| CloudConnexa API | Integrates with other systems to manage your WPC programmatically, automate workflows, and more |
| IaC using Terraform | Automates your CloudConnexa configuration, user management, access control, and more in the form of code to ensure consistency and ease scalability |

## Hear from our customers

“The implementation team at CloudConnexa was a cut above. They were able to precisely guide me in configuration of IPSEC VPN tunnels using Unifi gateways. The system has continued working very well, providing reliable inter-cloud connectivity using SD-WAN.” — Systems Administrator, Greypool

“The process of installing openvpn is simple and secure. Once loaded I can connect to [my clients’] systems whenever they need help…Their portal is clear and easy to understand. Customer support is also quick and helpful.” — Sam C., Small Business Director

“What I appreciate most is that every time the VPN is activated, the user must authenticate through Single Sign-On (SSO). This enables us to link all our critical systems to the VPN, and if necessary, we can easily revoke access by deactivating the user’s main account using the SSO.” — Chays V., Small Business Head of Operations


See what others are saying about CloudConnexa on G2.