ZTNA With

CloudConnexa

Attack Surface Minimized

CloudConnexa

Service is delivered using a software defined, multi-tenant, worldwide, virtual networking platform

30+ worldwide Points of Presence

Each region utilizes high-performance servers from multiple data-centers

Powered by our mesh core network

Kernel-optimized, high-performance OpenVPN core.
Gigabit Internet connections
Route diversity and reduced latency

Providing Wide-Area Private Cloud(s)

Multi-tenant network provides a dedicated virtual cloud network (Wide-area Private Cloud) immediately on-demand.

Technologies

- Complete separation of control and data plane with everything in software
- Control plane built using cloud-native technologies
- Data plane on bare-metal servers using kernel-optimized data forwarding
- Vertical integration of security and data forwarding stacks
- Multi-tenant service
- Full-mesh connected core network

Outcomes

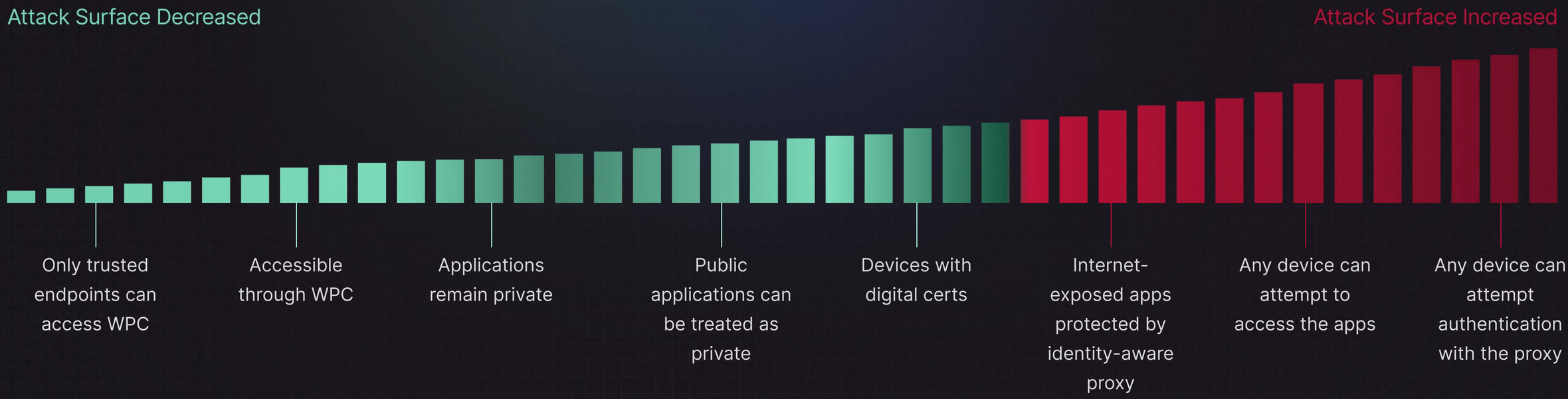
- Unlimited service scale
- Centralized network and security policy administration
- Distributed enforcement close to edge
- Instant creation of secure virtualized overlay networks
- Low latency, high performance connections with built-in security
- High availability and redundancy

What is ‘Attack Surface’?

“An attack surface is defined as the total number of all possible entry points for unauthorized access into any system. It includes all vulnerabilities and endpoints that can be exploited to carry out a security attack. The attack surface is also the entire area of an organization or system that is susceptible to hacking.”

https://www.techtarget.com/whatis/definition/attack-surface

Attack Surface



Zero Trust

Cloaking

- Services kept private to reduce attack surface
- No private network routes are leaked
- No incoming tunnel connections to networks
- PoPs terminate connections & protect from DoS

Segmentation

- Only authorized services available as routes
- Patent-pending domain routing segments by app
- Hosts can be used to access private apps and not the network
- Multi-WPC allows a WPC to be used to segment based on use case, department, privileged access
- Per-App firewalls only allow authorized protocols

Identity

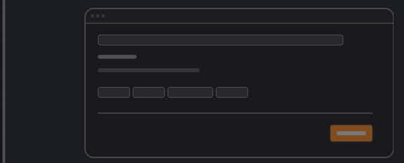
- Buit-in 2FA
- SSO using SAML, or LDAP
- Digital certs for IoT and unattended clients
- Access control for Networks, Hosts, and User Groups between each other and to applications and IP service segments

How to create ZTNA with CloudConnexa

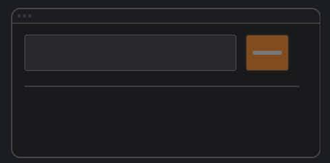
1. Create Wide-Area Private Cloud (WPC)
2. Define Trusted Applications & IP Services
3. Define Trusted Users & Devices
4. Define Access Policies
5. Shield against cyber threats

Create Wide-Area Private Cloud (WPC)

1



Signup for an account



Assign a Cloud ID to your WPC

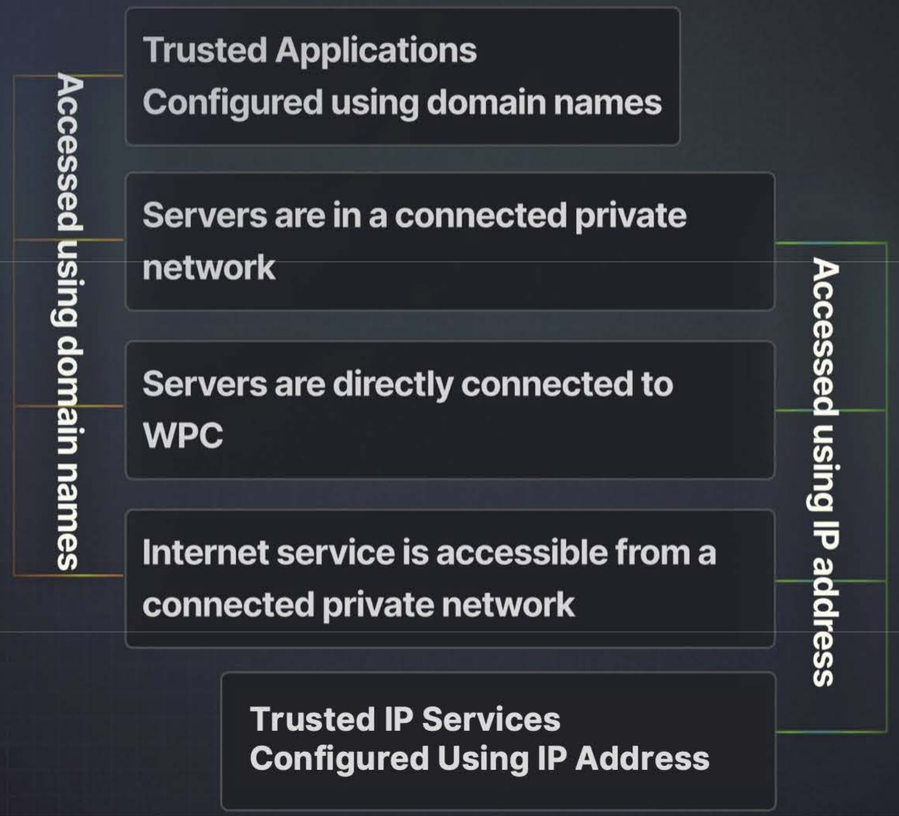
Your WPC is ready for immediate use

Define Trusted Applications & IP Services

Private Trusted Applications and IP Services are only accessible via the WPC. Traffic destined to internet accessible trusted destinations is routed via the WPC

Why configure select public internet services as trusted?

- Make them appear as private applications for access visibility and access control
- Use built-in IDS/IPS and add security by tunneling through untrusted internet access networks (e.g., Wi-Fi hotspots)
- Use SaaS login controls to allow logins only from trusted source networks
- Maintain end-to-end HTTPS integrity by using WPC route to bypass unneeded deep packet TLS inspection



Make Trusted Applications and Services Accessible

Deploy one or more Connector(s) on the networks hosting the trusted private applications or providing internet access to the trusted public services

Application Servers

Deploy one or more Connector(s) on the networks hosting the trusted private applications or providing internet access to the trusted public services

Deployment

Connector software can be deployed on light-weight VMs

Networks can be connected using OpenVPN compatible routers

Software Availability

Infrastructure as code templates can be used to quickly spin up Connectors on IaaS and VPS providers

Easy to use scripts

All desktop operating systems

Define Trusted Users and Devices

Users & User Groups

- Trusted Users are created automatically when Users successfully authenticate via federated authentication or LDAP
- Trusted Users can also be created manually and authenticated via password and 2FA
- User Groups are created manually and associated with users either manually or by mapping to LDAP and SAML attributes

Devices

- Limits can be placed on the number of devices per user
- Trusted devices are created automatically when a User authenticates and imports the connection profile on a device
- Trusted devices can also be manually created, and profile distributed to devices by other means
- Certificate-based authentication can be used for always-on unattended operation

Define Access Policies

- Role-based or least privilege access can be configured using Access Groups
- Access Groups let you enforce identity-based policies, so the users get access only to the trusted applications and IP services that they need
- Access Groups can also permit communications between User Groups
- Devices are sent IP address routes to only the authorized IP Services. This automatic micro-segmentation thwarts lateral movement
- Private IP addresses of trusted Applications are never exposed to the connected user. Keeping your applications and private network cloaked

Continuous Protection

5

Intrusions

- Preserves end-to-end TLS connections
- IPS rejects traffic that matches certain threat signatures

Cyber Threats

- DNS-based content filtering
- 43 Content Categories
- Protects against malware, ransomware, phishing, adware, cryptojacking among others

Data Loss and other threats

- Works alongside third-party cyber security providers

Untrusted Internet Traffic Routing Options

Split-Tunnel ON

Keep split-tunnel ON for a direct local ISP route to the internet protected by Cyber Shield content filtering

Use a third-party security solution in tandem to secure internet traffic

Split-Tunnel Off

Keep split-tunnel OFF to route via WPC to add Cyber Shield intrusion prevention

Route via WPC to a private network that serves as an Internet Gateway and protects using a third-party security stack

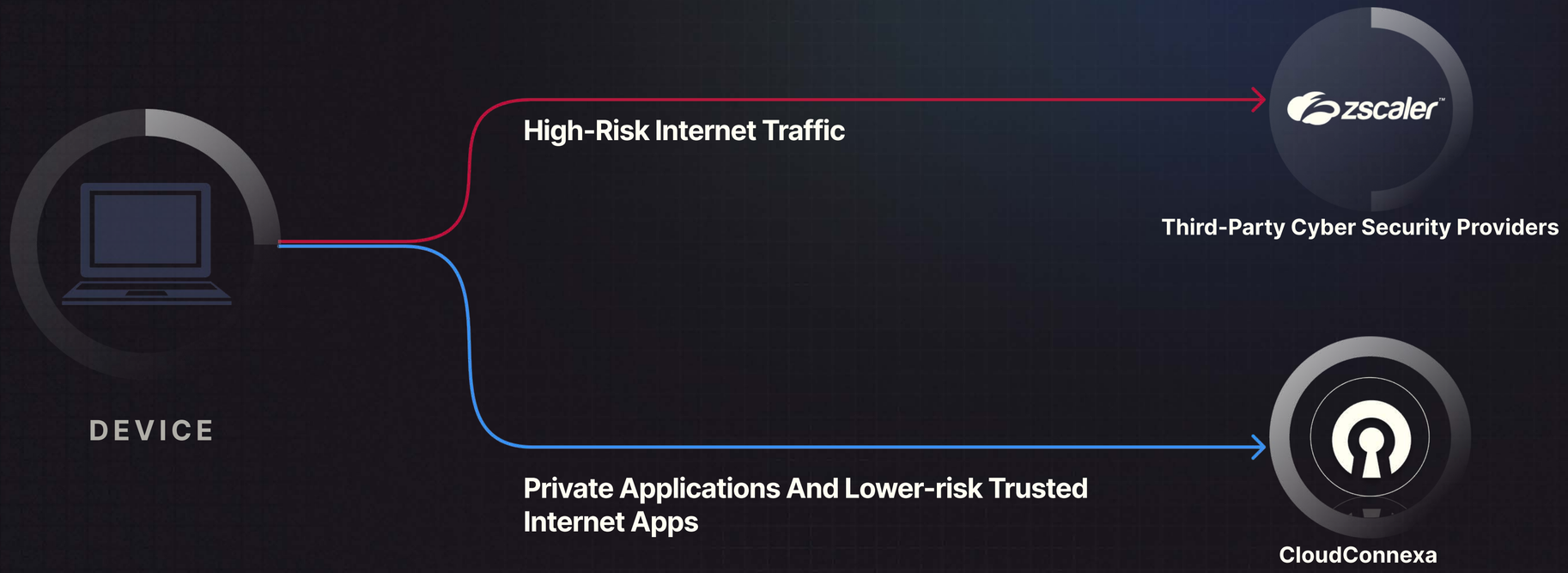
Restricted Internet

Block all untrusted traffic using restricted internet

A great solution for internet connected devices like digital kiosks, Point of Sales systems etc.

Working in tandem

Built in and extendable security features



ZTNA Differentiators

Segregation of trusted and untrusted traffic flows

Multiple options to secure untrusted internet traffic

Bi-directional Accessibility: Supports network-initiated flows and can also apply policies around it.

Restricted Internet Access: Locks down the device and allows it to only reach a set of authorized private and trusted public destinations.

ZTNA for IoT: IoT devices can authenticate using digital certificates and get access to applications based on identity-aware policies

ZTNA for Server to Server communications or API communications: Servers and other API originators or endpoints can be given a unique identity and therefore identity-based access policies.

ZTNA between Sites: Provides all devices on a network access to authorized applications hosted on a different network

Built-in security: Content filtering and IDS/IPS

Automatic network segmentation: Automatically segments the routes based on requesting entity's identity and access controls

Access to applications hosted on networks with overlapping IP address subnets

Protection of access to SaaS apps: Secures SaaS application access by tunneling traffic to those trusted application via a customer-owned internet gateway while allowing other internet traffic to use local direct internet access

Peer-to-Peer Communications: Enforces policies around whether a group of devices can communicate with each other or another group of devices directly

Self-service Scaling: On-demand scale the number of connections needed for ZTNA up or down with immediate effect.

Links & Additional Material

- Webinar: ZTNA is the new VPN
- Get Started with CloudConnexa
- Get Started with Zero Trust SaaS Application Access (CloudConnexa)
- How to configure CloudConnexa Restricted Internet Access
- CloudConnexa: Flexible Internet Routing
- CloudConnexa: ZTNA to Applications Hosted on AWS VPC
- Micro-segmentation for IP-Services
- OpenVPN Cyber Shield Traffic Filtering Introduction
- CloudConnexa Multi-Factor Authentication (MFA) Configuration

THANK YOU

CloudConnexa

ZTNA Made Easy