



PRESIDIO™

Cloudflare for CVS Health

In Partnership with Presidio

Secure Network Service Solution in Support of CVS Health's RFP for a Self-Service Consumable Third-Party Landing Zone (3PLZ)



CONFIDENTIAL

Prepared by Jake Seroussi, Cloudflare Client Director, CVS Health
V1, February 6, 2026

Project Objective

CVS Health is seeking to partner with Cloudflare and Presidio to design and deliver a connectivity solution in the form of a Third Party Landing Zone, that enables secure, isolated, and auditable access between external third parties (vendors) and CVS Health's enterprise applications.

As such, Cloudflare, Presidio, and CVS Health will partner to design a solution architecture that achieves the best elements of network security: least privilege, segmentation, intent, and identity.

This solution is intended to be largely automated and consumable as a self-service solution that can be directly consumed by application development teams, extending the DevOps philosophy of "build, run, own" into the delivery and consumption of network security.

Core Requirements:

- Standardized IPSec Connectivity
- Protects enterprise applications from external access
- Operates with split-brain proxy model for separate routing domains
- Granular Access Control
- Highly Available
- Streamlined onboarding with intuitive self-service portal
- Aligns with SOC 2, ISO 27001, and NIST standards for compliance



Cloudflare's connectivity cloud

A unified cloud platform uniquely powered by a global cloud network

Legacy network complexity holds back digital projects

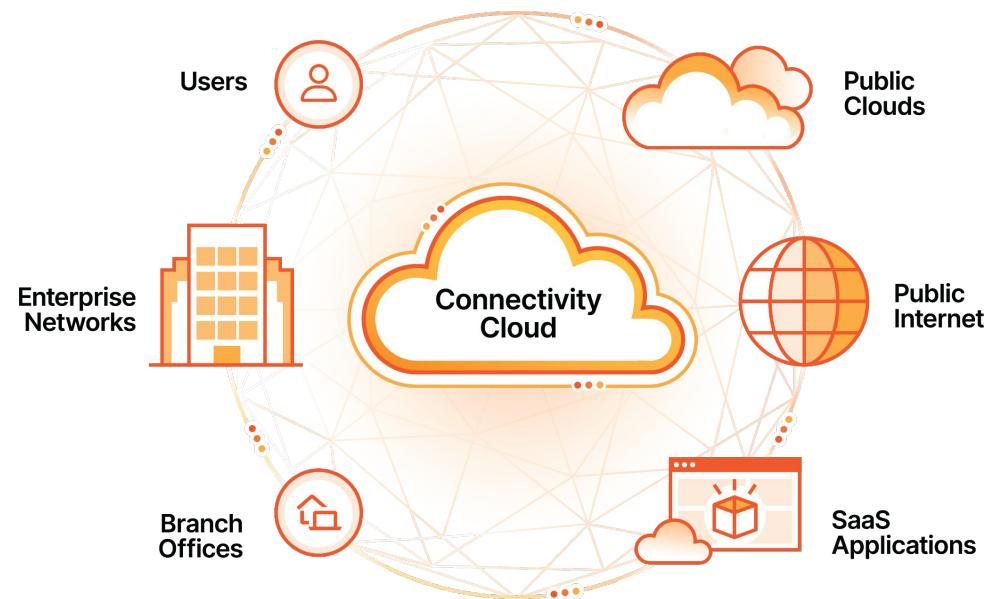


- User experience issues
- Security risk
- Fragile resilience
- Reduced agility
- Increased cost

Cloudflare's connectivity cloud resolves digital complexity

Cloudflare's connectivity cloud:

A unified platform of connectivity, security, and developer services powered by a programmable global network.



One network, one control plane on a global scale



330+ cities
in 125+ countries, including mainland China
w/ 210+ cities
for AI inference powered by GPUs



~20%
of web properties sit behind Cloudflare
including 80%
of the top 50 genAI companies



234 billion
cyber threats blocked every day



449 Tbps
of network capacity (and growing)

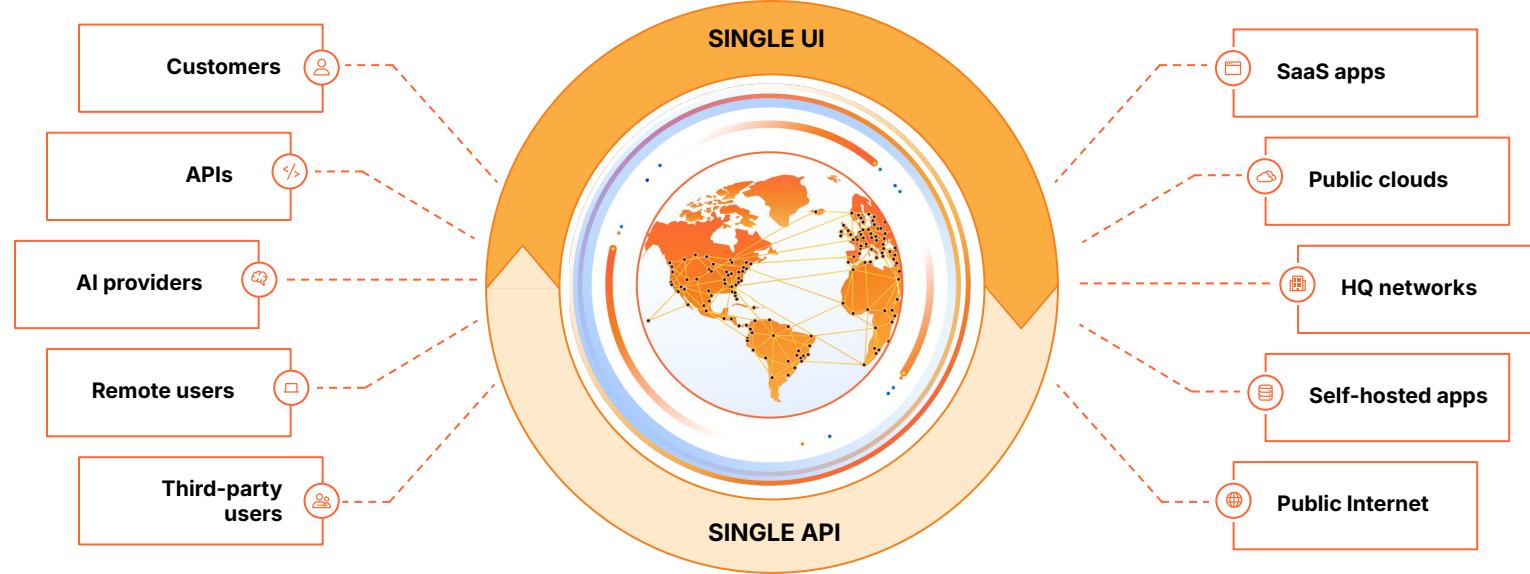


Unmatched network resilience



Simplified management interface

Log service integrations



Automation via Terraform

Composable, programmable services — Customizable for any use case



Customize Cloudflare services with **serverless code** that runs everywhere or anywhere



Keep using your existing **IP range**



Limit data processing and logging to **specific countries and regions**



Cloudflare's connectivity cloud

Connect.Protect.Build

 SASE & Workspace Security

- ZTNA (with MCP Server Portals)
- SWG (with AI Usage Controls)
- CASB (with AI Posture Management)
- Email Security
- Data Loss Prevention
- Remote Browser Isolation
- Digital Experience Monitoring

 App Security & Perf Services

- Firewall for AI
- Bot Management (with AI Crawl Control)
- WAF with Rate Limiting
- API Protection
- Load Balancing
- L7 DDoS Protection
- CDN and DNS
- Origin Shield

 Developer Services

- AI inference
- AI Gateway
- Agentic SDK and Workflows
- Serverless compute
- Full stack applications
- Object & key-value storage
- SQL database
- Media optimization and delivery

 Network Services

Network-as-a-Service Firewall-as-a-Service L3 & L4 DDoS Protection Network Interconnect Smart Routing IDS/IPS

Cloudflare Programmable Global Network

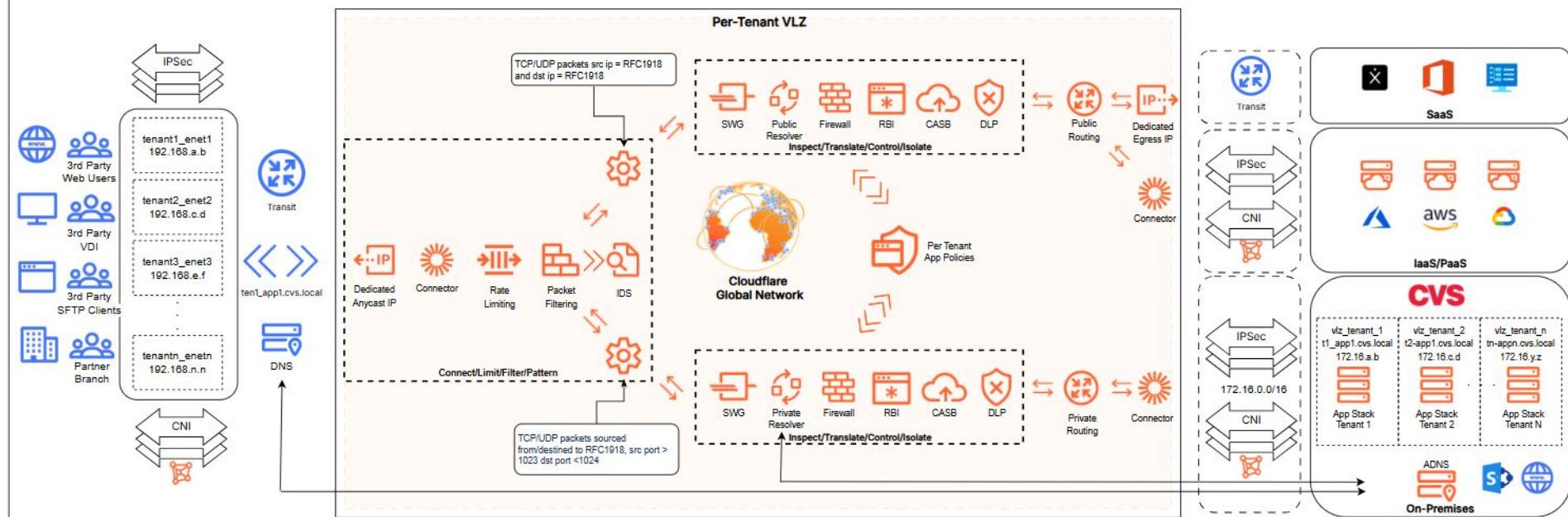


Artificial Intelligence/Machine Learning



Threat, Network Intelligence

Proposed 3PLZ Architecture



449 Tbps
of network capacity and growing

~50 ms
from ~95% of the world's Internet-connected population

234B
avg daily cyber threats blocked in Q3'25

~13,000 networks
Globally interconnected, including major ISPs, cloud services, and enterprises

~20-25%
of the web sites behind Cloudflare's network

330+ cities
in 125+ countries, including mainland China

Proposed Solution Set

Cloudflare Product Offerings as Made Available in Presidio Rate Card



Services	Capabilities and Impact
CDN	Edge content delivery: Ultra-fast static content caching and delivery via Cloudflare's global network, secured with SSL/TLS and protected by post-quantum cryptography.
Web Application Firewall (WAF)	Blocks attacks on web applications and APIs: Protect apps and APIs from zero-day vulnerability exploits, common attack techniques, use of leaked credentials, and more with rulesets powered by machine learning and threat intelligence.
Advanced DDoS	Cloud-native layer 7 distributed denial-of-service protection: Automatically detect and mitigate layer 7 DDoS attacks via our unmetered, unlimited, and autonomous DDoS protection systems.
Foundation DNS	Enterprise-grade managed DNS: Authoritative DNS service with advanced nameservers, zone-level DNS settings, unique DNSSEC keys, and enhanced analytics.
Advanced Certificate Manager	SSL/TLS certificates for web apps: Secure web applications and user data with TLS certificates (supporting PQC key agreements) that are automatically issued and renewed, reducing certificate lifecycle management overhead.
Bot Management	Detect and respond to bots: Identify and mitigate automated traffic to protect your web and mobile apps from bad bots based on bot scores. These scores are calculated based on machine learning models, heuristics, JavaScript detection, verified and AI bot categories, and mobile device verification signals.
Layer 7 Smart Routing (Argo)	Dynamic content delivery optimization: Automatically detect network congestion in real time and route traffic across the most efficient path over the Internet for optimal content delivery and user experience.
Advanced Rate Limiting	Traffic volume control based on any HTTP request characteristic: Limit the number of HTTP requests to apps and APIs made over a set timeframe based on any HTTP request characteristic — not just IP addresses — to block more sophisticated attackers. These limits adapt to changes in traffic patterns.
Payload Inspection	Inspect body data and headers: Inspect payloads that matched WAF rules to aid in incident response or inspecting WAF rule behavior.
API Security (API Shield)	Discover public APIs and protect APIs from attacks: Discover shadow APIs with machine learning models and protect them from business logic abuse and other attacks with a positive security model.

Continued... (2 of 3)

Services	Capabilities	Impact
ZTNA and SWG (Access and Gateway work together)	Granular context verification	Continuously verify identity, device posture, and other context to inform authorization decisions
	Per-resource Zero Trust policy enforcement	Enforce default-deny rules for all resources: SaaS and self-hosted apps, internal IPs and hostnames, and infrastructure targets
	Low-latency resource access	Eliminate VPN issues with cloud-native access controls that scale with your organization
	DNS and network filtering and HTTP/S inspection	Enforce security, app, and content categories; AV and sandboxing; and traffic and tenant rules — <i>plus, DLP profiles explained below</i>
	AI-backed threat intelligence	Block known and emerging threats using intelligence derived via AI models analyzing the vast amount of traffic on Cloudflare's network
	File sandboxing	Quarantine previously unseen files downloaded by your users into a sandbox and scan them for malware
CASB and DLP	API integrations (<i>beyond inline protection explained above</i>)	Analyze SaaS and cloud apps for misconfigs, exposed files, shadow IT, and suspicious activity to protect data and ensure compliance
	Discover and protect sensitive data across all services	Increase data visibility and prevent breaches, data exfiltration, and accidental exposure across web, email, and SaaS apps
NaaS (Magic WAN) and FWaaS (Adv Magic Firewall)	Site-to-site branch connectivity	Easily facilitate site-to-site connectivity across network locations like branch offices, retail locations, or factory floors
	Secure hybrid and multicloud connectivity	Centralized controls to route and secure traffic across varied public cloud environments and on-prem data centers
	Cloud-native layer 3 network firewall	Consistently enforce network security policies across your entire WAN, without backhauling traffic or creating choke points
	Intrusion detection	Expands the security coverage of your firewall to analyze and monitor network traffic against a broader threat signature database
	Included WAN traffic	In addition to not charging for user bandwidth, each user license helps you build your WAN fabric

Continued... (3 of 3)



Services	Capabilities	Impact
Load Balancing	Private network load balancing	With private IP support, get near real-time failover across multiple servers, whether they are deployed in a private, public, or hybrid cloud
Remote Browser Isolation (Browser Isolation)	Secure, low-latency remote browsing	Eliminates the risk of zero-day browser vulnerabilities and prevents users from loading malicious web content on their device
	Controlled user actions	Restricts keyboard input, file download/upload, copy/paste, and print functions to prevent users from leaking credentials and sensitive information
Layer 3 Smart Routing (Argo for Magic WAN)	AI-based smart traffic routing for best-path delivery	Optimizes your network performance and improves reliability using dynamic traffic intelligence from the Cloudflare network

Self-Service Portal Delivery

CVS Health 3rd Party Landing Zone Portal

Our Understanding

This initiative is a strategic modernization of CVS's third-party connectivity model, delivering a secure, automated, and self-service 3PLZ platform. The solution will replace manual, bespoke integrations with a standardized, policy-driven approach that enforces tenant isolation, least-privilege access, and identity-based controls by default. Through a simple portal and API, application teams will onboard partners without network expertise while maintaining compliance and reducing operational overhead. The program's success is defined by delivering a production-ready platform within one year, onboarding up to five initial partners, and establishing a scalable foundation capable of supporting enterprise-wide third-party connectivity at scale.

Key Assumptions

- CVS will provide executive sponsorship and timely decision-making
- A primary vendor will be selected and fully engaged for the duration of the program
- Existing CVS IAM, PKI, and SIEM platforms are available for integration
- Initial scope is limited to defined service patterns and up to five partner onboardings
- The platform will prioritize automation and self-service over custom integrations
- Security and compliance requirements are approved during design and remain stable through delivery

Solution Approach & Architecture

12 Month Breakdown of Activities and Outcomes by Phase

Activities	Design and Alignment	Platform Build & MVP	Pilot Onboarding	Scale Pilot & Transition
Months 1–2	<ul style="list-style-type: none"> Define portal workflows, RBAC, and approval gates Establish governance, roles, and success metrics Finalize reference architecture, tenant/VLZ model, and service patterns Align security, compliance, and operating model 	<ul style="list-style-type: none"> Build portal, APIs, and automation/orchestration layer Implement tenant/VLZ creation and IPsec "VPN to nowhere" Deliver DNS rewriting and initial service proxies (Web/API and generic TCP) Enable logging, monitoring, and SIEM integration 	<ul style="list-style-type: none"> Onboard first 1–2 pilot partners using self-service workflows Execute functional, security, and failover testing Refine portal UX, automation, and dashboards Develop and validate runbooks and support processes 	<ul style="list-style-type: none"> Onboard additional partners (up to 5 total) using standardized patterns Validate repeatability, onboarding SLAs, and minimal operational touch Complete production acceptance and security sign-off Define Year-2 roadmap and scale strategy
Outcomes	<ul style="list-style-type: none"> Approved end-to-end architecture and delivery plan Clear service catalog and onboarding workflows Security and compliance requirements locked Readiness to begin platform build 	<ul style="list-style-type: none"> Functional MVP platform in a production-like environment Automated, self-service tenant and tunnel provisioning First service patterns available for consumption Operational visibility and auditability established 	<ul style="list-style-type: none"> Successful onboarding of initial pilot partners Validated security, resilience, and operational model Refined platform based on real-world usage Operations team ready to support production use 	<ul style="list-style-type: none"> Up to five partners live on the platform Proven, repeatable self-service onboarding model Reduced manual effort and operational risk Scalable foundation ready for enterprise-wide expansion

Team Summary / Metrics

- Solution Owner | US**
- Application Architect | US**
- Sr. AppDev Principal Engineer | India**
- Sr. UI Designer | India (100% for 2 months)**
- 3 Engineers ***
- Sr. QA Engineer ***
- (*) Resources assignment and refinement will adjust as scope as the project matures
- All Resources shown are at 100% allocation unless otherwise stated

Price

Estimated Cost: \$2,032,000.00

(*) Pending refinement of scope as the project matures

Support Services

Support & Success Bundles

With you every step of the way

Curated support & success bundles to optimize your Cloudflare experience
the duration of your contract

Onboarding and optimization
workshops

Success planning and health
checks

More ways to connect with
tech support

Faster response SLAs



Standard & Premium options available

[Learn more](#)

Technical Account Management Benefits

Streamlined, expedited technical support

Single Point of Contact



- Centrally manages support across your Cloudflare products & services
- Provides proactive updates on issues, alerts, and during incidents
- Maintains detailed documentation of your technology stack and deployment

Globally Consistent



- Primary TAM available during in-region business hours
- Follow-the-sun TAM team monitors critical tickets
- Emergency hotline 24/7/365
- Multilingual options available

Priority Access



- TAM is available to answer questions and open tickets via email and private Slack channel
- 30 minute SLA for P1 issues
- Escalation management, frequent updates until resolution



Issue Tracking & Reports



- Recurring summary reports track issue status and support trends over time
- TAM offers comments and recommendations for improvement
- Custom root cause analysis delivered post event



[Learn more](#)

Cloudflare onboarding and implementation options

	Digital	Success	Professional Services		Partners
	Available to all	Premium	Quickstart packages	Migration/Expert	All options+
	Self-guided	SME-guided	Advisory	Advisory/hands-on	Advisory & Fully Managed
Product documentation	✓	✓	✓	✓	✓
Communities: Cloudflare + Dev	✓	✓	✓	✓	✓
Reference architectures	✓	✓	✓	✓	✓
Technical blog	✓	✓	✓	✓	✓
Entitlements review		✓	✓	✓	✓
Product feature overview		✓	✓	✓	✓
Optimization best practices		✓	✓	✓	✓
Use case development			Guided	Guided or hands-on	Guided or hands-on
Testing & validation			Guided	Guided or hands-on	Guided or hands-on
Configuration			Guided	Guided or hands-on	Guided or hands-on
Admin enablement			Guided	Guided or hands-on	Guided or hands-on
Multi-product deployments			✓	✓	✓
App/ZT/SASE deployments			✓	✓	✓
Network deployments			✓	✓	✓
Project management				✓	✓
Architectural design				✓	✓
Deployment execution				✓	✓
Performance fine tuning				✓	✓
Customized requirements				✓	✓
Complex use cases				✓	✓
Modernization consulting					✓
Third-party integration					✓
Fully managed services					✓

Digital resources



 <u>Community</u>	 <u>Docs</u>	 <u>Resource Hub</u>	 <u>Help Center</u>	 <u>Developers</u>
 <u>Blog</u>	 <u>theNET</u>	 <u>Cloudflare Radar</u>	 <u>CloudflareTV</u>	 <u>Connect</u>

Technical Support



Cloudflare experts

Support for all products & services



Globally available

Multilingual
x 7 x 365



Online resources

Knowledge base, dev docs & community forums

Support Portal | In-product access to how-to articles, smart diagnostic tests, self-service troubleshooting

Chat | Real-time chat

Phone Support | Emergency inbound, scheduled outbound

Community Forum | Connect with peers and experts, continuous knowledge share

How to Contact Support | Overview of support tiers and instructions on how to reach out

Thank You!