

Securing federal growth and the Qualys workforce on one platform

Two Cloudflare proposals for Nate Smolenski, Chief Information Security Officer. Each answers three questions: **why do anything**, **why Cloudflare**, and **why now**.

PROPOSAL 1 · FEDERAL

Cloudflare FedRAMP

A faster, FedRAMP-authorized edge for the federal platform, and a foundation for the IL4 / IL5 roadmap.

\$183,753 / year

Replaces: OCI WAF* and the home-grown CDN*

Includes: CDN, WAF, API Shield, rate limiting, Workers, R2

PROPOSAL 2 · WORKFORCE

Zero Trust, Email & AI Governance

One platform to see user activity, govern shadow AI and stop data loss, replacing three point products.

\$225,530 / year

\$9.40 per user / month (2,000 users)

Replaces: Cisco Umbrella*, Cisco AnyConnect*, Proofpoint

BOTH PROPOSALS · TOTAL ANNUAL INVESTMENT

\$409,283 / year

Already in place: Cloudflare serves qualys.com today and Zero Trust seats are already contracted.* Both proposals extend a platform Qualys already runs.

THE THREE QUESTIONS AT A GLANCE

	WHY DO ANYTHING?	WHY CLOUDFLARE?	WHY NOW?
Proposal 1 Cloudflare FedRAMP	Federal is growing, but OCI has no CDN and its WAF is a management burden. The home-grown CDN hurts performance and competitiveness.*	CDN, WAF, API Shield and rate limiting in one FedRAMP environment, on a platform Qualys already runs in production.	IL4 / IL5 is the long-term goal. Edge decisions made now shape what has to be built, assessed and defended later.
Proposal 2 Zero Trust, Email & AI	No visibility into end-user activity, and no controls over shadow AI, GenAI spend or data loss. A top concern for the company.*	Three point products become one platform, one agent and one policy engine, with CASB, DLP, RBI and AI Gateway included.	GenAI adoption is outpacing policy. Every month unmanaged is a month of AI usage nobody can see.

* Per account-team input; not publicly observable. See "How we know" and methodology on the final page.

Cloudflare FedRAMP

Replace OCI's WAF and the home-grown CDN with a FedRAMP-authorized Cloudflare edge for the Qualys federal platform.

1 Why do anything?

Federal growth is exposing the gaps in the current stack.

- ✓ Federal customers are a growing, strategic focus for Qualys, and they expect the same speed and protection as commercial.*
- ✓ OCI's WAF is a management burden. Engineering time goes to operating it instead of improving the product.*
- ✓ OCI has no CDN, so Qualys runs a home-grown one. Its performance problems make Qualys less competitive.*
- ✓ The gap has shown up in past proofs-of-concept. It is a big reason Qualys has already expanded its use of Cloudflare.*

Competitive context: federal is one of the most contested segments for Qualys, primarily against Tenable.*

2 Why Cloudflare?

One FedRAMP-authorized edge, already proven inside Qualys.

- ✓ CDN, WAF, API Shield and Advanced Rate Limiting on one platform. It retires both the OCI WAF and the home-grown CDN.
- ✓ Already in production: qualys.com is served by Cloudflare today (public DNS and HTTP evidence), and Qualys has grown its footprint since past POCs.
- ✓ Inheritable controls for the roadmap. Authorized edge services let Qualys inherit controls instead of building and evidencing its own, the groundwork for IL4 / IL5.†
- ✓ Workers and R2 on the same platform for federal-specific logic and storage at the edge.

† Authorizations are granted to Qualys by the relevant authorizing bodies. Cloudflare's federal team can map inherited controls with Qualys' assessor.

3 Why now?

Decide the edge before the boundary is locked in.

- ✓ Federal is a stated company priority and the pipeline is growing. Each federal POC on today's stack repeats the same performance story.*
- ✓ IL4 / IL5 is a multi-year effort. The CDN and WAF choices made now decide how much Qualys must build, document and defend later.*
- ✓ The home-grown CDN is a standing engineering cost and a standing risk, and both compound every quarter.
- ✓ Fastest time to value: same vendor, same account and same tooling Qualys already runs commercially.

Decision window: the sooner the edge is on Cloudflare, the sooner federal POCs are won on performance instead of explained away.

PROPOSAL 1 · ANNUAL INVESTMENT

\$183,753 / year

REPLACES
OCI WAF + home-grown CDN*

Included: CDN, WAF, API Shield, Advanced Rate Limiting, DNS, Workers, R2, Zero Trust Suite and Premium Success. Full scope on the next page.

What Qualys gets, and what standing still costs

SCOPE — CLOUDFLARE FEDRAMP ENVIRONMENT

COMPONENT	SCOPE
FedRAMP environment	Authorized boundary for all services below
CDN	1 TB data transfer · 10 MM requests
Application security	WAF · Advanced Rate Limiting · API Shield
DNS	10 MM queries
Domain & certificates	1 Enterprise domain (qualys.us) · Advanced Certificate Manager (1) · Custom SSL (15)
Developer Platform	2 Workers · R2 object storage (100 GB)
Zero Trust Suite	500 seats
Premium Success	Included
Total annual investment	\$183,753 / year

COST OF STANDING STILL — ILLUSTRATIVE

RISK FACTOR	ASSUMPTION	ANNUAL IMPACT
Lost or delayed federal deals	\$10M federal pipeline, with ~10% put at risk by current-stack limitations*	\$1,000,000
Home-grown CDN upkeep	2 dedicated engineers at ~\$200K fully loaded each*	\$400,000
Security & performance risk	Service disruption, delayed signature or patch delivery, or an incident	Unquantified
Estimated annual cost of inaction		~\$1,400,000

COST OF INACTION / YEAR

~\$1.4M

CLOUDFLARE FEDRAMP / YEAR

\$183,753

ESTIMATED RETURN

~7.6x

Please pressure-test these numbers. The pipeline, at-risk percentage and CDN engineering cost are account-team assumptions and have not been verified against Qualys' actual figures. Replace them with yours and the return recalculates. Even with the pipeline impact removed, the CDN engineering cost alone is ~2.2x the annual investment.

DECISION REQUESTED

Approve **\$183,753 / year** for the Cloudflare FedRAMP environment, and schedule a technical workshop with the federal platform team to confirm cut-over sequencing and map inherited controls for the IL4 / IL5 roadmap.

Zero Trust, Email Security & AI Governance

Replace Cisco Umbrella, Cisco AnyConnect and Proofpoint with one Cloudflare platform that sees user activity, governs shadow AI and prevents data loss.

1 Why do anything?

The workforce is a blind spot, and AI made it bigger.

- ✓ There is no clear visibility into what end users are doing: which apps they use, which sites they visit, what data moves.*
- ✓ Shadow AI: employees are using GenAI tools with no sanctioned path and no inventory.*
- ✓ No GenAI controls over spend, and no DLP on prompts or uploads. For a security company, that is a real exposure.*
- ✓ Three point products (Cisco Umbrella*, Cisco AnyConnect*, Proofpoint), each with its own console, policy and renewal.

Priority: a top concern for the company right now.*

2 Why Cloudflare?

One platform, one agent, one policy engine.

- ✓ Zero Trust (2,000 seats), CASB, DLP, Remote Browser Isolation, AI Gateway, Email Security (3,000 seats) and PhishGuard in one package.
- ✓ One DLP policy set. AI Gateway DLP reuses the same detection profiles as Cloudflare One, so web, email and AI prompts are covered by one definition of sensitive data.
- ✓ AI Gateway adds guardrails, logging and usage controls across AI providers, which answers the shadow-AI and spend questions directly.
- ✓ Builds on what exists: Zero Trust seats are already contracted* and Cloudflare already fronts qualys.com.

Net effect: fewer vendors, fewer consoles and one set of logs for the security team.

3 Why now?

AI adoption is moving faster than policy.

- ✓ Every month without controls is a month of AI usage nobody can see, measure or limit.
- ✓ It is a live corporate concern. The fastest answer is extending the Zero Trust deployment already in place, not starting a new vendor evaluation.
- ✓ Consolidation lowers cost: about \$9.40 per user per month for the full stack (2,000 Zero Trust users), against an estimated \$17 to \$33 for the equivalent point products (page 6).
- ✓ Share the Cisco and Proofpoint renewal dates and we will sequence the cut-over so there is no coverage gap.

Same relationship: pairs with Proposal 1 under one Cloudflare agreement and one team.

PROPOSAL 2 · ANNUAL INVESTMENT

\$225,530 / year

PER USER

\$9.40 / user / month

Replaces Cisco Umbrella*, Cisco AnyConnect* and Proofpoint. **Adds** CASB, DLP, Remote Browser Isolation, AI Gateway and PhishGuard.

What is in the package, and what it costs per user

THE PACKAGE

CAPABILITY	SCOPE	WHAT IT DOES FOR QUALYS
Zero Trust Access, Gateway, WARP	2,000 seats 1,000 contracted today*	REPLACES Cisco Umbrella* (secure web gateway / DNS filtering) and Cisco AnyConnect* (remote access)
CASB	Included	NEW Visibility and control over SaaS apps, sanctioned and unsanctioned
Data Loss Prevention	Included	NEW Detect and block sensitive data in web traffic, SaaS and AI prompts
Remote Browser Isolation	Included	NEW Isolate risky sites and unmanaged-risk browsing away from endpoints
AI Gateway	Included	NEW Shadow-AI visibility, guardrails, DLP on prompts, usage and spend controls
Email Security	3,000 seats	REPLACES Proofpoint (public MX / SPF records point to Proofpoint today)
Email PhishGuard	Included	NEW Managed phishing detection and response from Cloudflare analysts
Total annual investment		\$225,530 / year

COST PER USER

PER USER / MONTH

\$9.40

\$225,530 ÷ 2,000 Zero Trust users ÷ 12

PER USER / YEAR

\$112.77

Everything in the package, per Zero Trust user

PER USER / MONTH, 3,000 BASIS

\$6.26

If spread across all 3,000 users and email seats instead

CAPABILITIES

7

Zero Trust, CASB, DLP, RBI, AI Gateway, Email, PhishGuard

How per-user is calculated. The headline uses the larger, more conservative denominator of 2,000 Zero Trust users, with email, DLP, CASB, RBI, AI Gateway and PhishGuard all included in that one figure. Spreading the same \$225,530 across 3,000 users and email seats gives \$6.26 per user per month.

Cloudflare vs. the point-product path

Estimated annual cost of Cisco + Proofpoint across all 3,000 users, plus the standalone DLP and CASB products Qualys would need to add to close the visibility and GenAI gaps.

LINE ITEM	BASIS	LOW \$/USER/MO	LOW / YEAR	BENCHMARK \$/USER/MO	BENCHMARK / YEAR
Cisco Umbrella*	3,000 users	\$2.50	\$90,000	\$4.50	\$162,000
Cisco AnyConnect*	3,000 users	\$2.50	\$90,000	\$3.50	\$126,000
Proofpoint email security	3,000 mailboxes	\$6.00	\$216,000	\$15.00	\$540,000
Standalone DLP (add-on)	3,000 users	\$3.00	\$108,000	\$5.00	\$180,000
Standalone CASB (add-on)	3,000 users	\$3.00	\$108,000	\$5.00	\$180,000
Estimated point-product total			\$612,000		\$1,188,000
Cloudflare — everything above, plus RBI, AI Gateway and PhishGuard			\$225,530		\$225,530
Estimated annual savings			\$386,470		\$962,470
Reduction vs. point products			63%		81%
Three-year savings, if held flat			\$1,159,410		\$2,887,410

PER USER — 3,000-USER BASIS

	LOW ESTIMATE	BENCHMARK ESTIMATE	CLOUDFLARE
All-in cost per user per month	\$17.00	\$33.00	\$6.26
All-in cost per user per year	\$204.00	\$396.00	\$75.18
Cloudflare, conservative: spread over 2,000 Zero Trust seats only	—	—	\$9.40 / mo \$112.77 / yr

A note on these numbers. These are modeled estimates based on typical enterprise pricing for a company of Qualys' size, not Qualys' actual contract values and not committed quotes. "Low" assumes deep volume discounts; "Benchmark" reflects typical negotiated pricing (the Proofpoint line uses a \$15 per user per month enterprise-bundle benchmark). Cisco and Proofpoint lines represent current spend, with all Cisco seats and the add-ons sized at 3,000 users*; DLP and CASB lines represent the standalone products Qualys would add to close the gaps*. Cloudflare Zero Trust is quoted at 2,000 seats while the Cisco estimate covers 3,000, so Cloudflare per-user is shown both ways. Remote Browser Isolation, AI Gateway and PhishGuard are **not priced** in the comparison, so it understates the gap. Share the actual Cisco and Proofpoint figures and renewal dates and Cloudflare will produce a custom TCO.

The combined investment

PROPOSAL	REPLACES	ANNUAL INVESTMENT
1 · Cloudflare FedRAMP	OCI WAF*, home-grown CDN*	\$183,753
2 · Zero Trust, Email & AI Governance	Cisco Umbrella*, Cisco AnyConnect*, Proofpoint	\$225,530
Total, both proposals		\$409,283 / year

RECOMMENDED NEXT STEPS

- 1
- Confirm scope.** Validate seat counts (2,000 Zero Trust, 3,000 email) and the FedRAMP service limits.
- 2
- Share current contracts.** Cisco and Proofpoint values and renewal dates, so we can replace the estimates with a custom TCO and plan a gap-free cut-over.
- 3
- Federal workshop.** Technical session with the federal platform team on CDN and WAF cut-over and IL4 / IL5 control inheritance.
- 4
- Shadow-AI baseline.** Run an observe-only discovery on the Zero Trust seats already contracted*, so the AI-usage picture is on the table before any policy is enforced.

YOUR CLOUDFLARE CONTACT

Andrew Geiser
Cloudflare
ageiser@cloudflare.com
(415) 990-5973
[linkedin.com/in/andrewgeiser99](https://www.linkedin.com/in/andrewgeiser99)

HOW WE KNOW

Cloudflare already fronts qualys.com
server: cloudflare · cf-ray response header

Cloudflare authoritative DNS
seth.ns.cloudflare.com · tara.ns.cloudflare.com

Cloudflare address space
apex A / AAAA in CLOUDFLARENET (ARIN)

Proofpoint
MX *.pphosted.com · SPF include:spf-001ca501.pphosted.com

Microsoft 365 (outbound)
SPF include:spf.protection.outlook.com

***Per account-team**
OCI WAF and home-grown CDN · Cisco Umbrella · Cisco AnyConnect (3,000 seats) · Zero Trust seats contracted · FedRAMP High and IL4 / IL5 roadmap · federal priorities and competitive context · cost-of-inaction assumptions

Methodology — no assumptions. Current-state vendors (Cloudflare and Proofpoint) were identified from public DNS records and HTTP response headers for qualys.com; lookups were performed on 26 Oct 2026 and should be re-run before sending. Network facts (Cloudflare address space, Cloudflare nameservers) are from public ARIN and DNS data. Items marked * (OCI WAF and CDN, Cisco Umbrella and AnyConnect and their 3,000-seat count, contracted Zero Trust seats, FedRAMP High and IL4 / IL5 plans, federal priorities, and the cost-of-inaction assumptions) are per account-team input and have not been independently audited; please confirm with Qualys. Cisco, Proofpoint, DLP and CASB costs on page 6 are modeled estimates, not Qualys contract values. Cloudflare does not itself confer Qualys’ authorizations; IL4 / IL5 and FedRAMP determinations rest with the relevant authorizing bodies. Pricing is annual and subject to the executed order form. Prepared by Andrew Geiser, Cloudflare. This proposal is not affiliated with or endorsed by Qualys.