ILLUSTRATIVE SAMPLE, SYNTHETIC DATA. Example Co. is invented, and so is every domain, name, ID, token, and value.

CLOUDFLARE CONFIGURATION REVIEW · FINDINGS REPORT

SYNTHETIC DATA

Cloudflare Security Review: Example Co.

Know what your Cloudflare security settings actually protect, and what still needs attention.

Account `XXXX-XXXX` Zones **example.com, example.org, example.net** Review date `XX/XX/2026`

Reviewer **SDS security team**

Scope and method

Read-only · human-checked

41 configuration checks run against the account	**8 of 9** outside-in checks ran. Proving DKIM needs a real email header.	**0** changes made. The token was read-only.	**15** findings, each checked and written up by a person

Findings at a glance

15 items

HIGH	MEDIUM	LOW	INFO	NOT VERIFIED
2	5	5	2	1

Most items are routine cleanup. "Not verified" means the read-only token could not see that setting. It is never counted as a pass.

How to read the evidence

Settings, not attacks

SETTING SEEN
We read this setting through the read-only token.

CONFIRMED OUTSIDE
Our public checks show the same thing from the internet.

NOT VERIFIED
The token couldn't see this setting. Check it by hand, or rerun the review with read access.

Every finding is an observed setting. None is a proven vulnerability, and none shows that anyone has misused it.

Fix these first

1. **API token with no expiry or IP limit.** It can change DNS and Workers. Add an expiry and an IP filter.
2. **AI Gateway without authentication.** It accepts requests with no gateway token. Turn on gateway authentication.
3. **MCP host partly outside Access.** One path has no Access login in front of it. Extend the Access app to cover it.

What we reviewed

Zones	3 (example.net is parked)
Public hosts	7, all proxied
Workers	site-router, chat-api, and forms-handler
AI Gateways	1 (gw-chat)
API tokens	4 (2 can make changes)

Please confirm this inventory on the walkthrough call.

All findings

15 items · sorted by severity

#	CHECK	WHERE	SEVERITY · EVIDENCE	WHAT WE FOUND	FIX
1	**Tokens that can make changes and never expire**	`ci-deploy`	HIGH · SETTING SEEN	This token can edit DNS and Workers on all zones. It has no expiry date.	Replace it with a narrower, expiring token. See detail A.
2	**AI Gateway without authentication**	`gw-chat`	HIGH · SETTING SEEN	Gateway authentication is off. Requests need no gateway token.	Turn on gateway authentication. See detail B.
3	**Tokens that can make changes with no IP limit**	`ci-deploy`	MEDIUM · SETTING SEEN	The same token has no IP filter, so it works from any IP address.	Limit it to your build server IPs. See detail A.
4	**AI Gateway with no rate or spend limit for the whole gateway**	`gw-chat`	MEDIUM · SETTING SEEN	No rate limit is set. Usage has no ceiling at the gateway.	Set a rate limit and a spend alert. See detail B.
5	**MCP or agent host not fully behind Cloudflare Access**	`mcp.example.com`	MEDIUM · SETTING SEEN	The Access app covers `/app` but not `/sse`.	Cover every path with Access. See detail C.
6	**Plain-text Worker variable named like a secret**	`chat-api`	MEDIUM · SETTING SEEN	A plain-text variable is named `API_KEY`. We recorded the name, never the value.	Move it to an encrypted secret, then rotate the key.
7	**DMARC policy weaker than reject**	`example.com`	MEDIUM · SETTING SEEN · CONFIRMED OUTSIDE	The policy is `p=none`, so it only monitors. Reports go to a mailbox you own.	Read the reports. Then move to quarantine, and later to reject.
8	**Minimum TLS version below 1.2**	`example.org`	LOW · SETTING SEEN · CONFIRMED OUTSIDE	TLS 1.0 and 1.1 are allowed. Our handshake test connected with both.	Set the minimum TLS version to 1.2.
9	**HSTS off**	`example.org`	LOW · SETTING SEEN · CONFIRMED OUTSIDE	Browsers aren't told to use HTTPS only. No HSTS header was sent.	Turn on HSTS with a short max-age first.
10	**Parked domain with no SPF or DMARC record**	`example.net`	LOW · SETTING SEEN · CONFIRMED OUTSIDE	It sends no mail, and it has no SPF or DMARC record.	Add `v=spf1 -all` and a reject DMARC record.
11	**No CAA record**	`example.com`	LOW · SETTING SEEN · CONFIRMED OUTSIDE	Any certificate authority can issue certificates for this zone.	Add CAA records for the authorities you use.
12	**Unused tokens**	`old-report-01`, `old-report-02`	LOW · SETTING SEEN	Two read-only tokens have not been used in over 90 days.	Confirm with the owner, then delete them.
13	**No MTA-STS and no TLS-RPT**	`example.com`	INFO · SETTING SEEN	Neither record exists. You won't get reports when encrypted mail delivery fails.	Add TLS-RPT first, then MTA-STS in testing mode.
14	**Wildcard DNS records**	`*.example.com`	INFO · SETTING SEEN	A proxied wildcard record points to your origin. It may be intended.	Confirm it is needed, or remove it.
15	**Account members without two-factor login**	`Account`	NOT VERIFIED	The token couldn't see the member list.	Check it in the dashboard, or add read access and rerun the review.

Severity guide: High: fix soon. Medium: plan a fix. Low: tidy up when convenient. Info: confirm it is intended.
Not verified: check by hand, or rerun with read access.

SYNTHETIC DATA

Detailed findings

Account-level items

A API token that can make changes, with no expiry or IP limit

Findings 1 and 3 — HIGH

WHAT WE FOUND

Token `ci-deploy` can edit DNS and Workers on all zones. It never expires, and it has no IP filter.

WHY IT MATTERS

A token like this works until someone deletes it. This finding does not show that it has leaked or been misused.

EVIDENCE (READ-ONLY API, SYNTHETIC VALUES)

```
token: ci-deploy   id: XXXX…XXXX   status: active   expires_on: (none)
policies: Zone.DNS:Edit, Workers Scripts:Edit (all zones)   ip_filter: (none)   last_used: XX days ago
```

FIX

Create a narrower token with an expiry and an IP filter. Update the build tool, then delete the old token.

FIX RISK · UNDO · CHECK AFTER

Low risk. Undo: keep the old token active until the new one works. Check after: the old token no longer shows as active.

B AI Gateway without authentication or a rate limit

Findings 2 and 4 — HIGH

WHAT WE FOUND

Gateway `gw-chat` accepts requests without a gateway token. It also has no rate limit for the whole gateway.

WHY IT MATTERS

Anyone with the URL could send requests billed to your AI provider account. This finding does not show that anyone has done so.

EVIDENCE (READ-ONLY API, SYNTHETIC VALUES)

```
gateway: gw-chat   account: XXXX-XXXX   authentication: off
rate_limiting: off   logging: on   called by: chat-api
```

FIX

Turn on gateway authentication. Add the gateway token to `chat-api` as a secret. Set a rate limit and a spend alert.

FIX RISK · UNDO · CHECK AFTER

Medium risk, because every caller needs the token before you turn this on. Undo: turn gateway authentication off. Check after: a request without the token is refused.

C MCP host partly outside Cloudflare Access

Finding 5 — MEDIUM

WHAT WE FOUND

An Access app protects `mcp.example.com/app`. No Access app covers `/sse` on the same host.

WHY IT MATTERS

Requests to that path skip the Access login. We did not test whether the app asks for its own login there.

EVIDENCE (READ-ONLY API, SYNTHETIC VALUES)

```
access_app: XXXX…XXXX   domain: mcp.example.com/app   policy: allow, group: staff
host: mcp.example.com   proxied: yes   paths with no Access app: /sse
```

FIX

Widen the Access app to the whole host, or add an app for `/sse`. Give MCP clients a service token.

FIX RISK · UNDO · CHECK AFTER

Medium risk, because MCP clients need the service token before you make the change. Undo: restore the old app domain. Check after: `/sse` asks for a login.

SYNTHETIC DATA

Not covered by this review

Stated up front

This is a configuration review. It is not a penetration test, a mail-tenant audit, or a guarantee that systems are secure.

- **Penetration testing.** No attacks, vulnerability scans, load tests, or login attempts.
- **SSL mode Full vs. Full (strict).** Not checked yet.
- **R2, D1, and Zero Trust Gateway policies.** Not checked yet.
- **Application code and MCP tool definitions.** AI checks look at configuration only.
- **App login and Turnstile.** We don't test whether they work in your app.
- **Inside Microsoft 365 or Google Workspace.** Mailbox rules, tenant policies, and admin settings need separate access.
- **AI tools your staff use outside Cloudflare.**
- **Other clouds, Microsoft 365 app secrets, and GitHub.**

Email: what a Cloudflare token can show

- **Checked:** SPF, DKIM, DMARC, MX, MTA-STS, and TLS-RPT records in DNS, plus Cloudflare Email Routing if used.
- **DKIM:** we found the Microsoft 365 DKIM selectors. Proving that mail is signed needs a real message header.
- **In this sample:** example.com has `p=none`, and parked example.net has no SPF or DMARC record.
- **Not checked:** anything inside the mail tenant. That needs separate access.

Authorization and token handling

- Before we ask for any access, we agree on scope with you in writing. We also give you a way to confirm you are dealing with SDS.
- The Cloudflare token is read-only. You can revoke it at any time.
- We walk you through how we handle the token before you create it.

Also in this report

Outside-in checks

8 of 9 ran. Public SPF, DMARC, and MX records match what Cloudflare holds. DNSSEC validates end to end.

Unproxied by design

1 record (autodiscover for Microsoft 365) is unproxied on purpose. It is listed separately and is not counted as a finding.

Each item includes

What we found, the evidence, how to fix it, how risky the fix is, and how to undo it.

Next steps

1. **30-minute walkthrough.** We go through the report with you and answer questions. You decide what to fix and when.
2. **Optional: guided fix help.** We guide your team on a screen share while your team makes each change. Each change has an undo step and a check after.
3. **Or fix them yourself.** Every item in this report includes the steps.

Read-only by default
We read settings. We don't change them.

You keep change authority
Your team makes every change.

Questions about this sample report?

ed@sdsitgroup.com · 754-357-8179

Illustrative sample, synthetic data. Example Co. and every name, domain, ID, token, and value here are invented. The domains example.com, example.org, and example.net are reserved for documentation. This is a configuration review, not a penetration test. A clean result does not mean systems cannot be compromised. Secure Data Solutions is not affiliated with or endorsed by Cloudflare, Inc.