WORKS WITH CLOUDFLARE · FINDINGS REPORT

SAMPLE · REDACTED

Cloudflare Security Review: Example Co.

This is a sample of the report you receive. All names, IDs, and values are fake or redacted. The layout, checks, and level of detail match a real review.

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

Reviewer **Eddie Espino**

Scope and method

Read-only · human-checked

41	9	0	15
configuration checks run against the account	outside-in verifications from the public internet	changes made. We used a read-only token with a 7-day expiry.	findings, each checked and written up by a person

Findings at a glance

15 items

2	5	5	2	1
HIGH	MEDIUM	LOW	INFO	COULD NOT SEE

Most items are cleanup, not emergencies. "Could not see" means the read-only token had no access. It is never counted as a pass.

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.** Anyone with the URL can send requests. Turn on gateway auth.
3. **MCP host partly outside Access.** One path skips the login. Extend the Access app to cover it.

What we reviewed

Zones	3 (1 parked)
Public hosts	7, all proxied but 1
Workers	worker-xxxx, worker-xxxx, worker-xxxx
AI Gateways	1 (gw-xxxx)
API tokens	4 (2 can make changes)

Please confirm this inventory on the walkthrough call.

Also in this report

Outside-in checks

9 of 9 ran. Public SPF, DMARC, MX, and CAA match what Cloudflare holds.

Unproxied by design

1 record (mail for Microsoft 365) is unproxied on purpose. It is listed apart, 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.

SAMPLE REDACTED

All findings

Sorted by severity

#	CHECK	WHERE	SEVERITY	WHAT WE FOUND	FIX
1	**Tokens that can make changes and never expire**	`token-xxxx`	HIGH	This token can edit DNS and Workers. It has no expiry date.	Add an expiry, or replace it with a narrower token. See detail A.
2	**AI Gateway without authentication**	`gw-xxxx`	HIGH	Anyone who has the gateway URL can send requests through it.	Turn on authenticated gateway. See detail B.
3	**Tokens that can make changes with no IP limit**	`token-xxxx`	MEDIUM	The same token works from any IP address.	Limit it to your office or build server IPs.
4	**AI Gateway with no rate or spend limit for the whole gateway**	`gw-xxxx`	MEDIUM	No rate limit is set. Usage has no ceiling.	Set a rate limit and a spend alert.
5	**MCP or agent host not fully behind Cloudflare Access**	`mcp.example.com`	MEDIUM	The Access app covers `/app` but not `/sse`.	Extend the Access app to cover every path.
6	**Plain-text Worker variable named like a secret**	`worker-xxxx`	MEDIUM	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 only none or quarantine**	`example.com`	MEDIUM	Policy is `p=none`. Reports are arriving, so you can see who sends as you.	Move to quarantine, then reject, in stages.
8	**Minimum TLS version below 1.2**	`shop.example.com`	LOW	TLS 1.0 and 1.1 are allowed. **Confirmed from outside.**	Set the minimum TLS version to 1.2.
9	**HSTS off**	`shop.example.com`	LOW	Browsers are not told to always use HTTPS. **Confirmed from outside.**	Turn on HSTS with a short max-age first.
10	**Parked domain that can still be spoofed**	`example.net`	LOW	It sends no mail, but it has no SPF or DMARC record.	Add `v=spf1 -all` and a reject DMARC record.
11	**No CAA record**	`example.com`	LOW	Any certificate authority may issue certificates for this zone.	Add CAA records for the authorities you use.
12	**Unused tokens**	`token-xxxx (2)`	LOW	Two tokens have not been used in over 90 days.	Confirm with the owner, then delete them.
13	**No TLS-RPT**	`example.com`	INFO	You get no reports when mail encryption fails.	Add a TLS-RPT record with a report address.
14	**Wildcard DNS records**	`*.example.com`	INFO	A 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`	COULD NOT SEE	The token had no access to the member list.	Check in the dashboard, or add read access and rerun.

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

SAMPLE · REDACTED

Detailed findings

Account-level items

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

HIGH

WHAT WE FOUND
Token `token-xxxx` can edit DNS and Workers on all zones. It never expires, and it works from any IP address.

WHY IT MATTERS
If this token leaks, it keeps working until someone deletes it. That makes it the most useful thing to tidy up.

EVIDENCE (READ-ONLY API, REDACTED)

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

FIX
Create a new token with only the needed zones, an expiry, and an IP filter. Update the tool that uses it, then delete the old one.

FIX RISK · UNDO · CHECK AFTER
Low risk. Undo: keep the old token active until the new one works. Check after: the old ID no longer lists as active.

B AI Gateway without authentication or a spend limit

HIGH

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

WHY IT MATTERS
Someone who finds the URL could run requests on your AI provider account. Your bill would show the usage.

EVIDENCE (READ-ONLY API, REDACTED)

```
gateway: gw-xxxx   account: XXXX-XXXX   authentication: off
rate_limiting: off   logging: on   called by: worker-xxxx
```

FIX
Turn on authenticated gateway. Add the gateway token to `worker-xxxx` as a secret. Set a rate limit.

FIX RISK · UNDO · CHECK AFTER
Medium risk, since callers need the token first. Undo: turn auth off. Check after: a request without the token is refused.

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: we help you fix items.** You approve each exact change in writing. Each one has an undo step and a check after.
3. **Or fix them yourself.** Every item above includes the steps.

Read-only by default
We look. We do not touch.

You keep change authority
No change without your written OK.

Questions about this sample? Email or call to see what a review of your account would include.

ed@sdsitgroup.com · 754-357-8179

SAMPLE · redacted. All names, IDs, tokens, and values in this document are fake. This is a configuration review, not a penetration test. A clean result does not mean systems cannot be compromised. "Works with Cloudflare" describes the platform we review; Secure Data Solutions is not affiliated with or endorsed by Cloudflare, Inc.