

Complimentary API Risk Assessment

Report prepared for **Example Company** as a thorough review of their API risk.

API security is paramount for GenAI, mobile apps, and SaaS platforms

58% of dynamic HTTP traffic on the Cloudflare network is API-related. All mobile app usage and GenAI integrations are driven by modern APIs.

Securing your GenAI-driven apps, mobile apps, and SaaS platforms requires protecting your APIs and apps at runtime and in real time. Customer trust is at stake, after all.

Built on our global, Internet-native network, Cloudflare API Shield automatically discovers, secures, and monitors API endpoints across your public landscape — without slowing business innovation. API Shield is natively integrated within Cloudflare Application Security, providing you with centralized web asset discovery, policy management, and analytics across your application security needs.

Our API Risk Assessment will discover your publicly accessible shadow APIs, their schemas, their context, and associated API risks. It will not disrupt your traffic and is compliant with your local data processing requirements, including PCI DSS v4.0, OWASP API Top 10, and New York State DFS guidelines.



Did you know?

Cloudflare's machine learning-based analysis found that **organizations underreport API endpoints by a factor of four**, as revealed in [2025 Cloudflare Signals Report](#).

Value of API risk assessment

Protect your customers' data

Build API endpoint baselines for acceptable sensitive data exposure. Identify when customer/user/organizational PII is unintentionally leaked, or when a greater than normal size of data is in the API response.

Know your attack surface

Discover API endpoints, their schemas, context, and purpose. Login, payment, and LLM APIs require different policies. Prioritize APIs based on risks associated with them (e.g., authentication, schema, response content and size misconfigurations).

Meet growing compliance standards

Help address compliance standards—including PCI, DORA, GDPR, other regional standards, and audit requirements—that require an inventory of public-facing assets and those that handle sensitive (PII) data.

Executive summary

Based on our discussions, we know that your organization is focused on strategic priorities such as expanding your mobile app presence, increasing critical apps' resilience, and providing improved customer experiences.

As you grow and add new technologies to your web properties, such as Generative AI and mobile apps, new attack surfaces emerge that can be used to compromise your users' data, inflate your infrastructure bills, degrade user experience, or compromise your web servers. Developers or website contributors often add functionalities to your apps that require integrations with third parties, often via APIs. These APIs are not always reported to security teams, leading to potential blind spots that can compromise your organization.

In collaboration with your team, we ran an API Risk Assessment on your account. We ran this assessment during the date range August 27 through September 5. During this period, we tracked that 70% of traffic to your assessed zones was API-related. We discovered a total number of 56 public facing endpoints.

Category	Total endpoints
Total discovered endpoints	56
GenAI / LLM API endpoints	2
Login endpoints	17
High risk endpoints	26
Medium risk endpoints	29
Low risks identified	1

Category	Total risks
Endpoint risks identified	100
High risks identified	20
Medium risks identified	35
Low risks identified	45

Category	Key statistics / Examples
Raw traffic volume for August 27 through September 5	webapp.cf-tme.com: 1,100,000,000 requests/month api2.cf-tme.com: 1,200,000,000 requests/month
Share of API traffic on monitored domains	webapp.cf-tme.com: 80% api2.cf-tme.com : 60%
Other prioritized API endpoints	webapp.cf-tme.com/admin-login/ api2.cf-tme.com/v1/llm-assistant api2.cf-tme.com/payment-info

How the assessment works

The best way to assess the effectiveness of security products is by using real-world data from your own websites. API Shield is an Internet-native service that runs within our Application Services reverse proxy, which enables us to provide real-time visibility and protection at runtime. With this deployment model, we set up this API Risk Assessment quickly, without deploying any hardware or software.

- We scanned your environment, with no impact on website performance or your end users. To minimize impact to your traffic, we did not deploy security policies to block or modify traffic as part of this assessment unless you specifically requested it.
- We ran an API Risk Assessment for you between **August 27** and **September 5**. You had immediate access to insights on discovered API endpoints and associated risks right after deployment.
- At the conclusion of the assessment, the Cloudflare team has provided a detailed, custom analysis. The assessment should be reviewed with your technical expert, **John Sharma**, and your account manager, **Asha Smith**. You can also access your dashboard at any time during the assessment.
- Additionally, your Cloudflare account team will alert you in real time to security risks to your public APIs or any active attack incidents we see during the assessment.

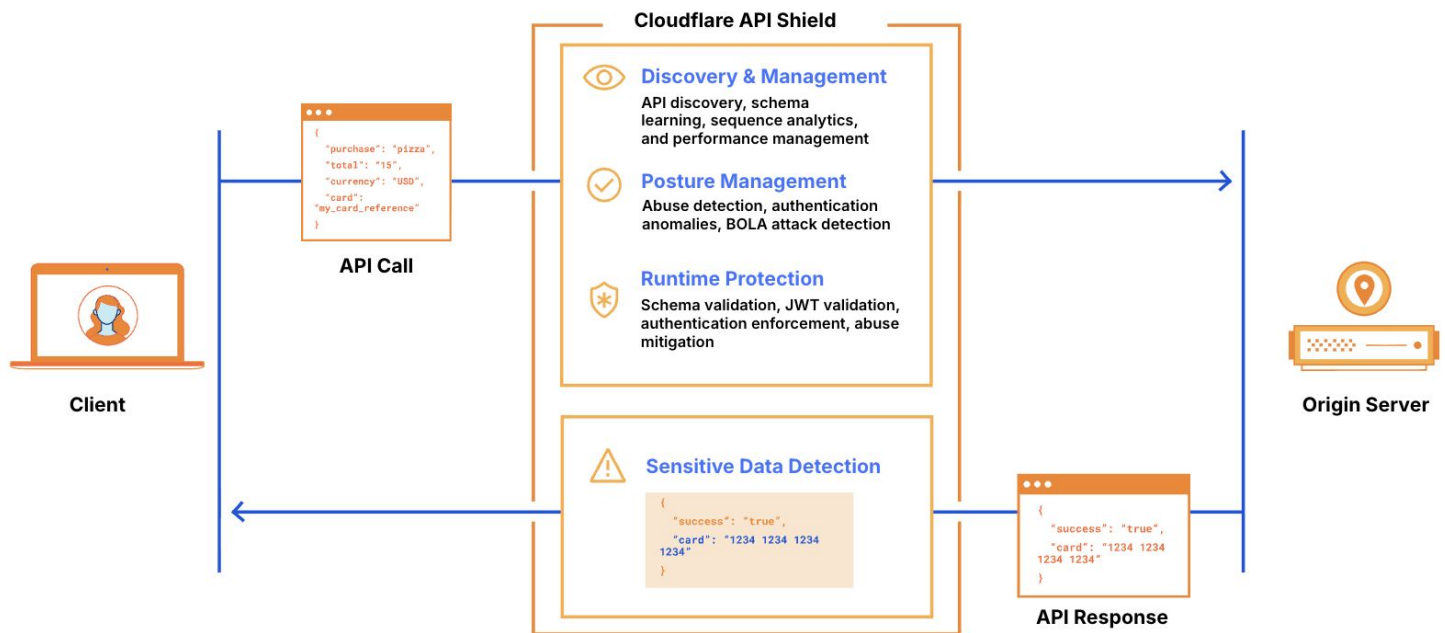


Figure 1: Cloudflare API Shield architecture

Assessment results - API discovery

Number of API endpoints discovered: 56

Sample of endpoints discovered:

- webapp.cf-tme.com/admin-login/
- api2.cf-tme.com/v1/llm-assistant
- api2.cf-tme.com/payment-info

Discovery [Learn more](#)

Automatically discover active API endpoints on your application. Save endpoints to Endpoint management for recommendations and analytics.

Discovered

Needs Review

Ignored

Hostname

57

2

2

6

Q Search...

Search

Show filters

Endpoint	Status	Source	
<div>/api/hello</div> <div>GET lb-api.cf-tme.com</div>	Needs Review	Machine Learning	<div>Save</div> <div> </div> <div>Ignore</div>
<div>/</div> <div>GET {hostVar1}.cf-tme.com</div>	Needs Review	Machine Learning	<div>Save</div> <div> </div> <div>Ignore</div>

1 - 2 of 2 items

Figure 2: Review the Discovery view under Web Assets tab in the Cloudflare Dashboard.

Assessment results - API misconfigurations

Endpoint counts by risk			
High risk	9	11	
	Broken (missing) authentication	Broken authorization (BOLA) - pollution and enumeration	
Medium risk	10	10	10
	Sensitive data returned	Missing API Schema	Broken (mixed) authentication
Low risk	15	15	15
	Response error anomalies	Response latency anomalies	Response size anomalies

Sample of API endpoints with one or more potential misconfiguration labels:

- [webapp.cf-tme.com/admin-login/](#)
- [api2.cf-tme.com/v1/llm-assistant](#)
- [api2.cf-tme.com/payment-info](#)

Endpoints

Discovery

Sequences

Schema validation

Client-side resources

Endpoints

Learn more

Secure your API endpoints and get recommendations and insights about your endpoint usage.

Export schema

+ Add endpoints

Q Search...

Search

Hide filters

Method

Hostname

Labels

All

All

4 items selected

Apply filters

Clear filters

Endpoint	Recommended rate limit per 10 min	Performance	Labels
<div><div>/v1/llm-assistant</div><div>POST api2.cf-tme.com</div></div>	Not enough session data	Errors: 99.84% Latency: No data	<div>cf-llm</div> <div>cf-risk-missing-auth</div> <div>+ 1 more</div>
<div><div>/v1/browse/new-releases</div><div>GET api.cf-tme.com</div></div>	<div>242</div> <div>Create rule</div>	Errors: 0% Latency: 2.1s	<div>cf-risk-mixed-auth</div>
<div><div>/v1/artists/{var1}</div><div>GET api.cf-tme.com</div></div>	<div>2.73k</div> <div>Create rule</div>	Errors: 1.1% Latency: 2.3s	<div>cf-risk-mixed-auth</div> <div>has-variable</div> <div>+ 1 more</div>

Figure 3: Review the Labels next to each API endpoint in the Endpoints view under Web Assets tab in the Cloudflare Dashboard.

Cloudflare's top recommendations to reduce API risks at Example Company:

1. **Protect against broken authentication and authorization (BOLA risks):** We found a high number of API endpoints with BOLA risks on your evaluated zones. We recommend implementing authentication (such as JSON Web Tokens, or JWTs) and authorization mechanisms that rely on user policies and hierarchy, and use random and unpredictable values as GUIDs for record IDs.
2. **Secure sensitive data in APIs:** 9 API endpoints on your zones returned sensitive data. We recommend deploying continuous monitoring for sensitive data detection. One option to consider is the Cloudflare Sensitive Data Detection Managed Ruleset in our WAF, which is integrated with API Shield and uses the same rules engine.
3. **Protect APIs with a positive security model:** As we found 7 endpoints that were missing API schemas, we recommend enforcing a strict, schema-based allow list for traffic. Use API schema learning to discover schemas for new or recently changed APIs. Then, validate schemas, authentication, and sequences.
4. **Safeguard shadow AI endpoints:** During our assessment, we discovered 2 unprotected GenAI / LLM API endpoints not previously reported to the security team. One option to protect these endpoints is to use Cloudflare's Firewall for AI module, currently in beta.
5. **Ensure all of your login endpoints are protected:** We recommend deploying multiple security controls for login endpoints. These include: Leaked Credential Check, Bot Management, Advanced Rate Limiting, and Sequence Mitigation. We also recommend that credential recovery/forgot password endpoints be treated as login endpoints.

Cloudflare API security resources

CLOUDFLARE

PRODUCT BRIEF

Cloudflare API Shield

Manage and secure the APIs that drive business

Modern API challenges

in a faster marketplace

APIs make the world go around. 56% of dynamic HTTP traffic on the Cloudflare Network is API related.

APIs present exciting business opportunities to deliver products faster and improve customer experience. None, security and IT leaders have to balance securing their APIs, on top of their web apps, without slowing down innovation.

Security and IT teams need to secure their customers' sensitive data while enabling business operations across web apps and API properties.

Customer trust is at stake, after all.

Cloudflare API Shield

Customers can discover, secure and simplify their public API security and management by consolidating their web application and API protection on the Cloudflare edge.

API Shield is part of Cloudflare's Application Security portfolio that also stops bots, threats DDoS attacks, blocks application attacks and monitors for supply chain attacks.

Shadow API risks

Design teams start when public web APIs without telling IT or APIs are connected to the

Authentication, data loss and abuse concerns

Once APIs are discovered, they could be abused from attackers

API performance monitoring

Given APIs drive business, once APIs are monitored and alerted, components must have

API Shield Product Brief

Directory
>
API Shield
>
Get started with API Shield

Page options
...

Get started with API Shield

This guide will help you set up API Shield to identify and address API security best practices.

Note

Enabling API Shield features will have no impact on your traffic until you choose to move a setting from `log` to `block` mode.

Session identifiers


While not strictly required, it is recommended that you configure your [session identifiers](#) when getting started with API Shield. When Cloudflare inspects your API traffic for individual sessions, we can offer more features for visibility, management, and control.

If you are unsure of the session identifiers that your API uses, consult with your development team.

Session identifiers should uniquely identify API clients. A common session identifier for API traffic is the `Authorization` header. When using a [JSON Web Token \(JWT\)](#) as the API for client authentication, its value may change over time. You can use a claim value inside the `JWT` such as `sub` or `email` as a session ID to uniquely identify the session over time.

If your API uses the `Authorization` header on more than 1% of successful requests to your zone, Cloudflare will automatically set it as the API Shield session identifier.

API Shield DevDocs



SOLUTIONS

The power of consolidated API protection


Modern application security requires an integrated
Gateway and Web Application Firewall (WAF)

APIs present a unique attack surface from web apps - from the very purpose of APIs in transferring data between systems to the variety of data formats.


With the fast growth in APIs, both behind modern web apps and as standalone external APIs, security teams are worried about API risks, sophisticated bots, client-side malware risks on top of web applications. The security risks with APIs include shadow APIs, authentication abuse, data loss, availability risks, and vulnerability exploitation.

Modern CISOs require an API Gateway integrated with the rest of their application security solutions - WAF, Bot Management, API-centric Rate Limiting and Client-Side Protection.


Customers and Analyst Recognition




2023 Gigamon Radar for Application & API Security
LEADER



2023 Forrester Wave for Bot Management:
STRONG PERFORMER



2022 Gartner Magic Quadrant for Web Application
and API Protection: **LEADER**



2020 OxBS Bot Management Market:

API Security vs Traditional WAF

Your Cloudflare account team



**Asha Smith,
Account Manager**



**John Sharma,
Sales
Engineering**



Sean Ming, Customer Success