TRACEABLE

Cloudflare vs Traceable

As a cloud services provider, Cloudflare offers a variety of products across application performance, CDN, network services, and application security. While Cloudflare is a mature cloud service provider, they are new to the API Security space with a loose collection of services based on traditional web application security technologies which are inadequate to fully protect against today's more sophisticated API attacks.

APIs and API Exploits are Different

APIs, API vulnerabilities, API attacks, and how you detect and stop them, are fundamentally different than yesterday's web application attacks. This is why OWASP, who produces the well respected OWASP Top 10 web app risks list, created an entirely separate list for APIs (OWASP API Security Top 10 list).

APIs often times have direct access to the data we need to protect and which the bad guys want. API attacks can take place over multiple transactions over a long period of time. Many API attacks consist of the threat actors using the API as it was designed, completely undetectable to WAFs and API gateways. Effective API security requires a contextual and behavioral understanding of the applications, their business logic, and user behavior. This requires constant deep data capture and ML analysis.

Traceable Value

Traceable delivers comprehensive API Security with an API Catalog with each API endpoint assessed for security posture, API security testing, API runtime protection, API abuse and fraud protection, and API threat analytics.

Discover

- Visibility of all APIs and their specifications (known, shadow, orphaned, 3rd party)
- Auto documentation of all APIs, including spec conformance analysis
- Per endpoint risk assessment, sensitive data visibility, drift management, and more

Protect

- Detection and blocking of OWASP API Security Top 10 and OWASP (web) Top 10
- Detection and alerting of sophisticated and long-running attack sequences
- Protect from API-specific attacks and API Abuse, including fraud and bots
- Testing of APIs for security vulnerabilities before they go into production

Analyze

- Identification of threat actors based on repeated malicious behavior
- Root cause analysis and threat hunting through explorable API transaction data lake

Comparisons

How do Cloudflare and Traceable compare for API security? Let's take a look.

	Cloudflare	Traceable
API Discovery	Cloudflare API discovery, a brand new functionality, requires a session identifier in the request header to discover an API. This can result in many missed APIs and incomplete discovery.	Traceable looks at all network traffic and reverse engineers APIs from request/response headers and bodies. This results in a complete and continuously updated inventory including auto OAS documentation.
API Visibility	Cloudflare can only see API traffic that goes through one of its edge services. This means it can only see North/South API traffic, which results in an incomplete inventory of your applications. You can't effectively secure your APIs if you can't see the whole application.	Traceable sees all the network traffic (North/South and East/West) because it offers the most flexible instrumentation options. Its distributed tracing foundation also connects the communications between them so you can see when internal (E/W) traffic becomes external (N/S) and have full application visibility.
API Protection	Cloudflare detection and protection of APIs is based on developer documentation. However, many API attacks use APIs as written, but in unexpected ways. Schema based protection won't catch these attacks	Traceable uses distributed tracing, deep data capture, and machine learning to detect and protect from known AND unknown attacks. Traceable correlates user behavior across time and sessions to protect from sophisticated hidden attacks.
Sensitive Data	Cloudflare scans response payloads for sensitive data. It can detect and blocks exfiltration of sensitive information in API responses.	Traceable tracks sensitive data and data sets, which are customizable. It not only can detect it anywhere in the API and block it, but also shows which API endpoints are handling it, which users are exfiltrating it, and what risk it is at.

Comparisons continued

	Cloudflare	Traceable
API Testing	Cloudflare does not offer any way to test APIs for vulnerabilities in pre-production or in production.	Traceable can run test sets on your APIs before production to find vulnerabilities and proactively resolve them. It will generate test traffic based on previous traffic. Traceable can also live scan your API traffic for vulnerabilities.
API Abuse, Fraud	Cloudflare covers API abuse by looking for anomalies in volumes of traffic going to each API, and by looking for sequence anomalies. But it only does looks at the edge (the WAF). It does not do anything to help find and stop cases of API fraud.	Traceable finds and stops API abuse and fraud by looking at volume, API usage behavior, and API user behavior. It also provides an explorable API transaction data lake of every transaction detail enabling forensics and threat hunting.
Rate Limiting, Bots	Cloudflare, through it's WAF, offers advanced rate limiting capabilities which can base rules on many different characteristics of HTTP traffic including request method, header, body, cookies, IP, country, ASN, and bot fingerprint.	Traceable has dynamic rate limiting with all the same capabilities and more, because it also understands APIs and their characteristics, and IP type (bot, TOR, VPN, etc). It also offers dynamic thresholds which can be set per API endpoint.
Conformance Analysis	Cloudflare provides conformance analysis (verifying that API documentation matches what is actually running) by not letting API calls through that don't match the specs. This will add maintenance overhead for developers and lead to reduced productivity.	Traceable provides conformance analysis by auto-documenting (in OAS format) all API specifications reverse engineered from live traffic. It compares to either the last capture or to developer docs and identifies shadow and orphaned APIs and parameters, and changes.
Root Cause Analysis, Threat hunting, Forensics	Cloudflare does not offer any tools to help with security incident root cause analysis, threat hunting, digital forensics, or even developer troubleshooting.	Traceable provides an explorable API transaction data lake with every transaction correlated and searchable by every criteria the system tracks, which enables root cause analysis, threat hunting, forensics, and troubleshooting.

Comparisons continued

	Cloudflare	Traceable
WAF	WAFs can protect against traditional web application attacks (OWASP Top 10), although often times with high false positives, but they only look at one transaction at a time and can't catch API business logic attacks like BOLA and mass assignment.	Traceable uses anomaly detection and ML to stop traditional web application attacks, with very low false positives, but also can stop business logic attacks. It can also integrate with your existing WAF to use it as a control point.
AuthN	Cloudflare requires mTLS to be set up and maintained in order to verify that proper authentication is happening. This requirement won't work for everyone, especially if they need to accept traffic from the unmanaged Internet.	Traceable uses sophisticated algorithms to identify properly authenticated APIs, and to identify and track authenticated users, regardless of changes to tokens, sessions, IPs, etc.
Performance and Observability	Cloudflare provides basic endpoint performance metrics such as request count, rate limiting recommendation, latency, error rate, and response size.	Traceable provides similar performance stats per endpoint and per service. But also, through its foundation of distributed tracing, it also provides complete visibility of how everything is connected, and exactly where and why there are errors or latency.

One Platform. One Solution.

If Traceable's capabilities sound amazing and comprehensive for API Security, that's because they are. And this is all in one platform, as one solution. Not a collection of tools that have been bundled together. Traceable has been built from the ground up to be a comprehensive API security solution.

Visit the Traceable website to learn more and to see a demo.