



The Truth About Cequence

Introduction

In today's rapidly evolving digital landscape, the security of your organization's APIs and applications is paramount. Meteoric growth in API use has brought along a corresponding rise in security risks – after all, APIs are highly-visible and well-defined doorways into an organization's data and business processes.

As cyber threats become more sophisticated, selecting the right security solution can make the difference between robust protection and vulnerability. At Cequence Security, we understand the complexities and demands of delivering a solution that scales from small enterprises to meeting the needs of the largest Fortune and Global 500 organizations. That's why we've developed a platform with a comprehensive array of solutions designed to cost-effectively safeguard your digital assets with unparalleled precision and effectiveness.

However, making an informed decision requires a thorough comparison of available solutions in the market. Unfortunately, not all vendors are earnest in their articulation of their own solution's capabilities, let alone how their competitors stack up. And while no vendor is perfect, we've seen wildly inaccurate information about Cequence on a particular competitor's web site.

This comparison sets the record straight, providing a detailed comparison between Cequence's actual capabilities, and those that we've seen vendors like Traceable incorrectly communicate. We offer a side-by-side comparison of Traceable claims and the truth, equipping you with the insights needed to choose the best solution for your organization's unique needs.

Whether you're concerned about API discovery, ensuring compliance, or enhancing your overall security posture including natively defending against attacks in real time, this comparison highlights the critical differences and advantages, helping you to make an informed, strategic decision.



Sequence API Security Strengths

The Sequence Unified API Protection (UAP) platform is the only security offering that addresses all phases of the API protection lifecycle, discovering an organization's entire API attack surface, eliminating unknown and unmitigated API security risks, and protecting its applications and APIs from cyber attacks that lead to data loss, fraud, and business disruption.

UAP continuously engages in complete discovery of your entire API attack surface, including internal, external, and third-party APIs, reveals your API risk posture pinpointing which critical security vulnerabilities need remediation, and provides real-time protection that detects and blocks attacks before they reach your applications. All without needing to modify or instrument your applications.

Complete Visibility

Sequence offers unparalleled visibility into your APIs, applications, and associated transactions. Its network-based deployment ensures the most comprehensive discovery and monitoring of APIs without relying on per-app instrumentation. Sequence integrates with existing infrastructure such as API gateways and CDNs in addition to deploying its own network sensor to identify API traffic. This unique combination ensures the broadest coverage possible, as well as the flexibility needed to protect applications and APIs independent of how and where they've been deployed.

Guaranteed Service Level Agreement (SLA)

Sequence offers high availability, offering zero-downtime upgrades that don't impact live application traffic or the end-user experience. We have the fastest speed of threat response across all API security vendors. And importantly, our inline deployment latency SLA is less than 15 ms (but usually hovers around the 5 ms mark).

Flexible Deployment

The number one barrier preventing organizations from achieving their desired state of protection for their web, mobile, and API applications is deployment difficulty. Unlike other vendors that require application modification or agents, Sequence is easily deployed passively or inline, across on-premises, cloud, or hybrid environments with no drama or required professional services engagements.

Dev/QA Cycles – No application modification using third-party code or some other agent. Who wants to add someone else's code to their app? This can be significantly time consuming, delaying time to value, often resulting in CPU/memory impacts for each app.

Compliance – Organizations want to know if the third-party code they're incorporating complies with their API specs/requirements. Is there a software bill of materials (SBOM) for any third-party code they will have to consume (a key building block in software security and software supply chain risk management)?

Performance – Of course, as applications slow down, end user dissatisfaction goes up. Instrumenting an app and forcing it to process bad traffic will only slow it down and result in customer dissatisfaction. Conversely, offloading bad traffic from an application that's been suffering under the load of attack traffic immediately improves its performance and reliability.

Cost – Bad traffic going to an app also disproportionately consumes CPU cycles and disk, increasing cloud costs.

Coverage – Sequence's network-level deployment ensures the greatest API and application coverage. This is in stark contrast to other API security solutions that require each application to be instrumented in order to be protected. And of course, not all applications can be instrumented. So solutions that support limited operating systems, application types, programming languages, or hosting environments are a partial solution requiring the organization to seek out additional tools for the apps not meeting those requirements.

Data Retention and Analytics

Vendors that rely on a data lake for attack identification and analysis are necessarily delayed in these objectives. Once their out-of-band analysis is complete, they require a third-party solution such as a Web Application Firewall (WAF) to perform any blocking. While Cequence supports long-term data retention (e.g., a data lake) as an add-on SKU, our ability to detect and mitigate threats in real time typically obviates the need for most organizations.

Native Mitigation

Unlike other vendors who can only mitigate issues by relying on a WAF, CDN, or API gateway, Cequence can natively mitigate attacks. These tools inherent limitations, such as the inability to block high-volume attacks and being dependent on easily-changed and easily-spoofed IP addresses, make them a suboptimal choice for API security. Cequence isn't limited by the number of allowed IP addresses, or the fact that the data must first travel to a data lake, be analyzed, then handed off to another piece of infrastructure. Cequence also provides several flexible mitigation options including logging, rate limiting, deception, and blocking.

Capabilities – The Truth

The tables below address Traceable claims made in their materials, detailing the truth for each item.

API Discovery	TRACEABLE'S CLAIM:  55%	THE TRUTH:	
		 100%	 70%
Discover & monitor edge API End-points (North-South APIs)	✓	Fully automated	Manual
Discover & monitor internal API End-points (East-West APIs)	✗	Internal, external, and third-party	✓
See into mTLS-encrypted API traffic without decrypting	✗	Fully supported with eBPF	eBPF ONLY
Auto grouping of discovered APIs into service/application collections	✓	✓	✓
Understand queries, parameters and attributes of the API	✓	✓	✓
Support for REST APIs	✓	✓	✓
Support for SOAP APIs	✗	✓	✓
Support for GraphQL APIs	✓	✓	✓
Discovery and tracking of 3rd party API and sensitive data use	✗	Supported with firewalls, web gateways, and eBPF	eBPF ONLY
Identify API changes and versions	✓	✓	✓

API Posture Management

TRACEABLE'S
CLAIM:

57%

THE TRUTH:


92%


64%

Discover and visualize API dependencies	✗	Q4 2024	✓
Discovery of sensitive data in the APIs	✓	✓	✓
Sensitive data classification into sets (including customized)	✗	Supports industry-specific sensitive data expressions	Generic ONLY
Discovery of sensitive data flows	✗	✓	✓
Flag shadow, zombie, and orphaned endpoints	✗	✓	✓
Automated risk scoring for API endpoints	✓	✓	✓
Ability to customize risk factors in API endpoints	✓	✓	✓
Automatically generate and download OpenAPI spec from runtime	✓	✓	✓
OpenAPI spec conformance analysis: runtime vs uploaded	✓	✓	✓
Per API endpoint vulnerability identification	✓	✓	✓
API posture change detection and alerting	✗	Risk events shown on UI and exportable	✓
Identify exposed APIs by external scanning	✓	Fully automated	Manual
Identify exposed credentials by external scanning	✓	Fully automated	Manual
Identify exposed vulnerabilities by external scanning	✓	Fully automated	Manual

Attack Protection

TRACEABLE'S
CLAIM:

64%

THE TRUTH:



100%



10%

Detect and block OWASP (Web) Top 10 security events	✓	✓	✓
Detect and block OWASP API Top 10 security events	✓	In real time	Delayed response
Detect and block newly-identified CVEs	✗	In real time	Delayed response
Detect and block API business logic attacks	✓	✓	Delayed & third-party ONLY
Detection of low & slow (long-lived, hidden) attacks	✗	In real time	Delayed response
Correlate threat actor (user) activity despite evasive tactics	✓	In real time	Delayed response
Automatically track the threat level of each user	✗	Identify threat actors by various attributes – usernames, sessions, fingerprints, IP addresses, and custom fields	Username ONLY
Pre-attack threat actor identification	✗	Identify threat actors by various attributes – usernames, sessions, fingerprints, IP addresses, and custom fields	Username ONLY
Identify and block abnormal API behavior (user behavior)	✓	Real-time, and using native and third party	Delayed & third-party ONLY
Identify and block abnormal API usage rates	✓	✓	Third-party blocking ONLY
Detect and block credential stuffing & brute forcing (ATO attempts)	✓	Native & third-party response	Third-party blocking ONLY
Detect and mitigate bad bots	✓	Native & third-party response	Third-party blocking ONLY
Detect and block application-layer denial of service (DoS) attacks	✓	Native & third-party response	Third-party blocking ONLY
Fully customizable protection policies based on transaction details	✓	✓	✓
Identify active data exfiltration per API, services, users	✗	Identify threat actors by various attributes – usernames, sessions, fingerprints, IP addresses, and custom fields	Offline analysis after the attack
Set and enforce sensitive data protection policies	✓	Supports industry-specific sensitive data expressions	Generic sensitive data

Attack Protection (continued)

TRACEABLE'S
CLAIM:

64%

THE TRUTH:


100%


10%

Enforce blocking in-line	✓	Native & third-party response	Third party ONLY
Enforce blocking by direct call to 3rd-party control points	✗	Native & third-party response	WAF blocking ONLY
Session integrity validation	✗	Session stitching can be done across different session IDs during a user journey	No session stitching
ML-based multi-dimensional and temporal fraud detection	✗	Custom Fraud Detection ML models, OOB rules and ML models and open system to incorporate customer models	Delayed detection
Customizable fraud detection rules and criteria	✓	Standalone dedicated fraud module deployed at the largest financial institutions	Delayed detection
Real-time fraud assessment	✓	Real-time detection and prevention	Not in real time

API Security Testing

TRACEABLE'S
CLAIM:

50%

THE TRUTH:


100%


90%

Test APIs for susceptibility to the OWASP
API Security Top 10



Flag API endpoint configurations not matching
industry best practices



We match industry best
practices AND org's
best practices by auto-
generating specs



Flag API endpoint configurations not matching
company policies



We can do this in testing
and production



Configure API tests without having OAS documentation



Zero-config API test configuration



Intelligent Mode allows
test plan generation
using OpenAPI specs or
Postman collections with
no added configuration



API input testing by generating inputs from known
bad payloads



UAP platform allows
for inter-solution
functionality between
Discover, Comply, and
Protect



White box security testing



Supports customizable
test cases and assertions
which allow security teams
to define custom test
criteria



Integration with external defect tracking



Provide API security tests for running in CI/CD pipelines



Provide remediation guidance for developers
and operations



Attack Detection and Threat Hunting

TRACEABLE'S
CLAIM:

56%

THE TRUTH:


90%


70%

Explorable transaction data lake	✗	Long-term data retention is an add-on SKU	✓
Analyze the body/payloads of requests and responses	✓	✓	✓
Detect suspicious client requests based on IP reputation	✓	Identify threat actors by various attributes – usernames, sessions, fingerprints, IP addresses, and custom fields	ONLY IP-based
Identify geolocation of API calls to help with API risk assessments	✓	✓	✓
Use IP Intelligence to assess API endpoint risk and set policy	✓	World's largest and fastest growing database of API threat intelligence	✓
API Performance metrics, call and error patterns	✓	✓	✓
Correlate and end-to-end connect all application API transactions	✗	Fully supported and goes beyond to allow security analysts to respond to analogies with a single click	No native response
Deep API transaction context for API incident response and threat hunting	✗	Fully supported and goes beyond to allow security analysts to respond to analogies with a single click	✓
Capture and store good, suspicious, and bad API traffic for analysis	✗	Both short-term and long-term (exportable) data available	Post attack data lake analysis provides no real-time protection
Share data with SIEM, SOAR, and ITSM systems	✓	✓	✓

Architecture & Deployment

TRACEABLE'S
CLAIM:

86%

THE TRUTH:

	
100%	43%
	
	CANNOT support enterprise-wide
	
Language/proxy independent	Language/proxy dependent
	
	Unproven on-premises deployments
Deployed at largest Telecoms and FinSerts	
	Air-gapped deployment unproven
Deployed at largest Telecoms and FinSerts	

Conclusion

Traceable’s architecture is a direct result of their application performance and availability monitoring roots (Traceable was launched in 2020 by the founder of AppDynamics). Their solution’s limitations are a bit easier to understand when looking through that particular lens. As such, it’s clear that the solution they offer today is a non-real-time API traffic monitoring and data analytics offering rather than a real API security solution. Their requirements for application instrumentation, reliance on a data lake for threat analysis, and inability to natively mitigate any found issues make the solution ill-equipped to protect a production application.

Cequence is the leader in API security and bot management. Our enterprise-grade security solutions are easily deployed without requiring development work or app instrumentation, offer actionability visibility across your applications and APIs, and are backed with a guaranteed SLA. Cequence Unified API Protection significantly improves visibility and protection while reducing cost, minimizing fraud, data loss, non-compliance, and business disruption. Learn more at www.cequence.ai.