TRACEABLE

API Security Solution Comparison Guide 2.0

This guide looks at what capabilities are needed to effectively secure your APIs in this new cloud, microservices, and API-driven application landscape, and then compares how a few API Security vendors rate against these criteria. The comparison data is sourced from as many public sources as we could find and represents our best understanding of the solution's abilities for each capability.



TRACEABLE

Overview

With the increased adoption of cloud-native applications, microservice architectures, and API-driven applications, APIs have become the critical glue that binds almost all the applications and online services that the world now uses daily.



What hasn't grown as quickly as API adoption is how we secure these critical communication channels. Most organizations are still attempting to secure APIs with traditional web protection technologies, unaware of the difference in risk that APIs introduce. Likewise, most application security solutions still focus only on traditional web vulnerabilities and not APIs. The threats from APIs are different, deeper, and often more difficult to detect and block. Hence, securing API-driven applications requires a new set of capabilities that are needed to have effective API security.

Key API Security Capabilities to Consider

APIs operate differently than plain web applications and present a far more complex surface area to secure. A primary reason is that they are not just the communication path carrying the business logic, but are often times themselves the business logic. This makes them far harder to secure, and far more dangerous if they are exploited. This increased complexity leads us to require far more sophistication in how we protect them. Hence, there are many capabilities to consider. We've broken them down into categories that align with the areas of API security that should be considered.

Categories of API Security

API Security encompasses a wide set of needs that often fall across different roles, teams, and products. Organizing the API security requirements into value-based categories helps to keep the conversation focused on what value each category provides its users.

At a high level, the value-based categories of the framework are:

- API Discovery
- Secure API Development
- API Security Posture
- API Security Insights
- Runtime Protection
- Architecture & Deployment



API Discovery

- **Discover API Endpoints in the system** - Discovery of all API endpoints in your application landscape. Enables users to be aware of their full exposure and all potential areas of risk.

- **Auto grouping of discovered APIs into service/application collections** - The auto grouping of discovered APIs into service/application collections. Uplevels many APIs into business logic and/or logical collections for enhancement of user comprehension and efficiency in the policy application

- **Understand queries, parameters, and attributes of the API -** Capture details about queries, parameters, and attributes of all the API endpoints. Enables users to fully understand API structure and areas of risk. Enables deeper and more thorough detection of malicious payloads.

- **Interpret REST, SOAP, gRPC, and GraphQL protocols** - Interpret REST, SOAP, gRPC, and GraphQL protocols. Enables the ability to detect anomalies and malicious behavior using the most highly used API protocols.

- **Discovery of 3rd party API use and configuration** - Discovery of 3rd party API use and configuration. Enables secure connections to and from 3rd party APIs. Important because 3rd party APIs are inherently riskier due to lack of ownership and less visibility.

- **Identify API changes and versions** - Identify changes in API definition, configuration, and versions. Alerts users to important changes which might affect the security of the API.

- **Discover & visualization of API dependencies** - Provides a live view of API requests, and data flow between services across your entire application environment.



API Security Posture

- **Discovery of sensitive data in the APIs** - Discovery of sensitive data in the APIs like credit card numbers, billing information, etc

- **Sensitive data classification (including customized)** - The ability to classify sensitive data into categories so that they can be handled appropriately. This should include the ability to customize classification criteria.

- **Discovery of sensitive data flows** - The ability to show what API endpoints sensitive data is going through, from the data perspective.

- **Flagging shadow, zombie, and orphaned endpoints** - Alerting on the discovery of APIs that live outside the normal IT governance management and security processes, APIs that were previously valid and approved but eventually abandoned or replaced

- **Ability to create collections and apply policies to them** - The ability to create collections and apply policies to them. Collections can consist of APIs, services, applications, etc. Enables more efficient policy setting and abstracted views for better understanding.

- **Ability to manually flag high-risk factors in API endpoints -** A per endpoint calculated risk score.It should be based on the likelihood of a breach and impact of a breach. Enables prioritization of mitigations and should roll up to services and applications.

- **Automated risk scoring for API Endpoints -** Ability to calculate risk score, without any manual interventions. It should be based on likelihood of a breach and the impact of a breach. Enables prioritization of mitigations and should roll-up to services and applications

- **Automatically generate and download OpenAPI spec from runtime** - Ability to generate an OpenAPI Specification compliant representation of all APIs seen in runtime, and download the spec for documentation and future use.

- **OpenAPI spec conformance analysis: runtime vs uploaded** - Compare runtime derived spec vs uploaded specs. Identifies mismatches in documentation vs runtime, pointing to potential security blind spots.

- **Per API endpoint vulnerability identification** - Scan, detect, and display, for each endpoint, all vulnerabilities that are found in each API endpoint being used at runtime. Helps with risk assessment.

Runtime Protection

- **Correlate threat actor (user) activity despite evasion tactics** - Ability to continuously track and correlate threat actor (user) activity across multiple transactions over time despite changes to IPs, sessions, and tokens.

- **Automatically track the threat level of each user** - Automated tracking of each user threat level based on their activity over time. This is the measure that turns users into threat actors. Can be used to determine user blocking.

- **Pre-attack threat actor Identification** - Idenify threat actors by their malicious, anomalous activity which is often reconnaissance and prelude to an attack. Requires accurate user activity storylining.

- **Detect and block OWASP Top 10 events** - A holistic API security solution should be able to detect and block the top vulnerabilities identified in the OWASP Top 10 (web), which focuses on web-based vulnerabilities.

- **Detect and block OWASP API Top 10 events, including session-based** - An effective API security solution must be able to detect and block the top API-based vulnerabilities identified in the OWASP API Top 10.

- **Detect and block newly identified CVEs** - Able to detect and block recently-discovered CVE's to ensure quick protection from new threats. Should have at least configurable detection to add new CVEs. Better if auto-loading at least daily.

- **Identify and block abnormal API behavior (user behavior)** - Ability to distinguish normal user behavior and abnormal behavior based on API consumption. And block malicious API consumption attempts.

- **Identify and block abnormal API usage rates -** Ability to distinguish between normal API usage rates and abnormal usage rates and block abnormal ones.

- **Detect and block credential stuffing & Brute forcing (ATO attempts)** - Detect and block any automated attacks attempting to achieve an account take over (ATO) by flooding the interface with sequences of credential guesses.

- **Detect and block bad bots use of the APIs** - The ability to block known identified bad bots from using the APIs of protected applications. This is distinct from detecting and blocking general bad bot-like behavior.

Runtime Protection

- **Detect and block bad bots use of the APIs** - The ability to block known identified bad bots from using the APIs of protected applications. This is distinct from detecting and blocking general bad bot-like behavior.

- **Detect and block application-layer denial of service (DoS) attacks** - DoS and DDoS attacks are typically volumetric attacks at the network layer, but application-layer DoS attacks operate at the API layer, looking to disrupt proper API responses to valid requests.

- **Enforce protection in heterogeneous environments** - It is important to be able to detect and block applications that span across on-prem, cloud, and hybrid environments, as most organizations have a mix of different environments.

- **Enforce blocking in-line** - Supports API security blocking directly through its own agents or other in-line software that is part of the single platform (i.e. not 3rd party integrations). Enables immediate blocking of attacks on detection, ensures blocking happens as expected, and reduces the complexity of configuration and maintenance.

- **Enforce blocking via integrations** - Supports API security blocking through integrations with external control points, such as API Gateways, WAF, proxies, etc. Enables out-of-band detection to inform blocking rules.

- **Identify APIs and services from which data is being exfiltrated** - Tracks and displays API endpoints and services that data is being exfiltrated from. Should give information to aid in prioritization and stopping of the exfiltrations.



Secure API Development

- **Flag API endpoint configurations not matching industry best practices** - Compare API endpoint configurations with industry best practices to highlight APIs which do not follow. Eg. Sensitive data shouldn't be passed in API URL, APIs should use encryption, secure coding practices for API dev.
- **Flag API endpoint configurations not matching company policies** - Compare API endpoint configurations with company policies to highlight APIs which do not follow. Eg. internal API calls should stay within their given geo, all authentication must happen through Okta, etc.
- **Pro-active vulnerability detection/probing using a library of known bad payloads -** Proactive vulnerability detection, probing, using a library of known bad payloads. This is like a more precise buzzing.
- **White box security testing** - Specific type of testing that use preserved credentials to test use cases that require proper authentication and provides much more information on the inner workings of their environment than it is required for a typical gray box **testing.**.
- **Integration with external defect tracking** - Ability to create a ticket for known vulnerabilities and track it in your system by integration with the API Security tool.
- **Provide API security tests for running in CI/CD pipelines** - Provide the ability to run API security tests from pre-production CI/CD pipelines. Enables shift left testing of APIs.
- **Can be integrated into CI/CD pipeline to effect pipeline behavior** - API Security posture aspects (eg. risk scores, test results, usage details) can be integrated into a CI/CD pipeline to help drive pipeline behavior.
- **Provide remediation guidance for developers and operations** - With every vulnerability that is found, include remediation guidance to aid developers and/or operations folks who will be asked to fix the found issues. Because most developers are not security experts.



API Security Insights

- **Analyze the body/payloads of requests and responses** - The ability to see the body/payload content of transactions is necessary to fully track and understand attacks and/or malicious behavior.

- **Detect suspicious client requests based on IP reputation** - Visibility on the reputation of IPs accessing and attacking your applications. This is not a suspicious geography, but more looking for specific IPs of known questionable integrity.

- **Identify geo-location of API calls to help with API risk assessments** - Identify and assess problematic patterns originating from known questionable geographical areas. Helps inform API risk assessments, either manually or automatically.

- **API Performance metrics, call and error patterns** - Visibility of the API performance metrics, call and error patterns. Insights on the availability and performance of API, API endpoints, and the validity of their data exchanges.

- **Correlate and end-to-end connect all application API transactions** - Track and correlate how API calls across the application runtime are related to each other. Includes external and internal calls, and how they connect together. This end-to-end transaction visiblity enables the most complete user tracking across entire sessions and hence full incident analysis capabilities.

- **Deep API transaction context for API incident response and threat hunting** - Collects header and bodies of request/responses, as well as API transaction sequences of all transactions, good and bad, to enable incident response, forensics, and threat hunting.

- **Share data with SIEM, SOAR, and ITSM systems** - Ability to share data with SIEM, SOAR, and ITSM systems to contribute to gaining greater overall security insights across all security disciplines being managed.

Architecture and Deployment

- **AI/ML based security and anomaly analysis** - Because of the number and complexity of APIs and their business logic, and the amount of data that they produce, AI/ML is required to effectively search for malicious patterns as well as to detect new ones.

- **Agentless (Mirroring, out-of-band)** - An out-of-band agentless deployment means that data collection is achieved without requiring any application code changes and that there is no agent in the path of the application communications. Typically performed via cloud traffic mirroring, or pod or daemonsets mirroring in Kubernetes.

- **Agentless (Edge - proxies, gateways, mesh)** - An edge agentless deployment means that data collection is achieved through adding a plugin/configuration to existing infrastructure, such as an API gateway, a load balancer, proxy, or a Kuberneties mesh.

- **Agent-based (language-specific, In-line)** - A deployment option that uses an in-app agent which sits in line with the application. In-app agents are typically libraries that can be linked in at runtime without code alteration. Typically inline/agent-based deployments can provide deeper system-level insights for better overall visibility and control points for more direct application protection.

- **Platform backend offered as SaaS offering** - The platform backend is made available as a SaaS offering where the vendor runs and manages the back-end solution, but the customer can still install data collectors in their datacenter or cloud.

- **Backend deployment on customer prem/cloud (self managed, air gapped)** - The platform backend (with data analysis, ML, admin control, etc) is available to be customer self-managed and air-gapped either on customer premises or in a customer cloud account.

Overall Scores

The overall percentage scores are based on the number of API Security capabilities each solution met according to our analysis, divided by the number of API Security capabilities (53).



Salt Security - 60%
Noname - 70%
Traceable AI - 96%

The sections below provide a deeper dive into each of the above 3 solutions based on the API Security capabilities.

TRACEABLE

Salt Security - 60%

Salt Security is an API security company based in Palo Alto, California. Salt Security provides an API protection platform to prevent attacks, using machine learning and AI. Deployed in minutes, the platform learns the granular behavior of a company's APIs and requires minimal configuration or customization to identify and block API attackers.

API Discovery	
Discover all API Endpoints in the system	✓
Auto grouping of discovered APIs into service/application collections	✗
Understand queries, parameters and attributes of the API	✓
Interpret REST, SOAP, gRPC, and GraphQL protocols	✓
Discovery of 3rd party API use and configuration	✓
Identify API changes and versions	✓
Discover and visualize API dependencies	✗
API Security Posture	
Discovery of sensitive data in the APIs	✓
Sensitive data classification (including customized)	✓
Discovery of sensitive data flows	✗
Flagging shadow, zombie, and orphaned endpoints	✓
Ability to create collections and apply policies to them	✗
Ability to manually flag high-risk factors in API endpoints	✗
Automated risk scoring for API Endpoints	✗
Automatically generate and download OpenAPI spec from runtime	✓
OpenAPI spec conformance analysis: runtime vs uploaded	✓
Per API endpoint vulnerability identification	✓
Runtime Protection	
Correlate threat actor (user) activity despite evasion tactics	✗
Automatically track the threat level of each user	✗
Pre-attack threat actor Identification	✓
Detect and block OWASP (Web) Top 10 security events	✗
Detect and block OWASP API Top 10 security events	✓
Detect and block newly-identified CVEs	✓
Identify and block abnormal API behavior (user behavior)	✓
Identify and block abnormal API usage rates	✓
Detect and block credential stuffing & Brute forcing (ATO attempts)	✓
Detect and block bad bots use of the APIs	✗

Salt Security (continued)

Runtime Protection (continued)	
Detect and block application-layer denial of service (DoS) attacks	✓
Enforce protection in heterogeneous environments	✓
Enforce blocking in-line	✗
Enforce blocking cia integrations	✓
Identify APIs and services from which data is being exfiltrated	✗
Secure API Development	
Flag API endpoint configurations not matching industry best practices	✗
Flag API endpoint configurations not matching compan	✓
Pro-active vulnerability detection/probing with a library of known bad payloads	✗
White box security testing	✗
Integration with external defect tracking	✓
Provide API security tests for running in CI/CD pipeline	✗
Can be integrated into CI/CD pipeline to effect pipeline behavior	✗
Provide remediation guidance for developers and operations	✓
API Security Insights	
Analyze the body/payloads of requests and responses	✓
Detect suspicious client requests based on IP reputation	✓
Identify geo-location of API calls to help with API risk assessments	✓
API Performance metrics, call and error patterns	✓
Correlate and end-to-end connect all application API transactions	✗
Deep API transaction context for API incident response and threat hunting	✗
Share data with SIEM, SOAR, and ITSM systems	✓
Architecture & Deployment	
AI/ML based security and anomaly analysis	✓
Agentless (Mirroring, Out-of-band)	✓
Agentless (Edge - proxies, gateways, mesh)	✓
Agent-based (language-specific, In-line)	✗
Platform backend offered as SaaS offering	✓
Backend deployment on customer prem/cloud (self managed, air gapped)	✗

Some things to investigate when considering Salt Security

API Discovery & Visualisation of API Dependencies

Maintaining accurate, up-to-date API inventory is critical to understanding potential risk and exposure. An outdated inventory results in widening the attack surface and creating more blind spots for your security teams. A continuous API discovery helps to identify and catalog all API endpoints, functions, and API parameters etc. Automated API discovery, API inventory, and classification of all APIs used by your applications, including shadow APIs, make it easy for you to be aware of changes and evolving risks.

Ideally, every vendor should have API dependency mapping and related visualizations as part of their API discovery capabilities. This capability should shed light on the data flow between services across application environments and provide a live view of all API requests. API dependency visualization provides actionable visibility for developers and security operation teams in Root Cause Analysis (RCA) and faster remediation.

Auto Grouping

Automatic grouping of APIs based on application type, sensitive data, services, business group, functional characteristics, etc. Auto grouping of APIs helps in improving the operational efficiency of security teams. It also helps in ease of policy enforcements to achieve faster governance and compliance objectives.

Automated API Endpoint Risk Scoring

When we talk about an API what we are really talking about is the collection of endpoints that comprise the API. A single API can have tens or even hunreds of API endpoints, each one presenting a potential attack surface. And each endpoint will have its own characteristics which factor into how risky it is for it to cause a breach. Given this, consider how incredibly valuable it is to not just have an inventory of all your APIs, but also some way to prioritize them according to how much risk they pose to your application security. An overall API security posture rating for the whole set of APIs which rolls up a score based the total number of vulnerabilities will not be granular enough to focus team efforts. To quickly identify the top risky API endpoints from the potentially hundreds or thousands that will likely be in your inventory it's important to have a per endpoint risk score.

Additionally, the factors that should be included in the risk score analysis will constantly be changing across the set of API endpoints. This means that the risk score really needs to be automatically and continuously calculated to give up to date assessments. When looking at API endpoint risk scoring solutions, make sure that the scores can be calculated automatically, as manual risk tracking will quickly become stale.

Sensitive Data Flow and Classification

Maintaining an API catalog that classifies sensitive data, like PII, PCI, PHI, PCI-DSS, etc is essential in quickly identifying and mitigating data breaches. You should look for a solution that has the ability to identify which services, API endpoints, and users are using your sensitive data. Knowing how your sensitive data flows across your services and APIs enables you to identify insecure or vulnerable APIs that could lead to devastating data breaches.

Runtime Protection

Business Logic attacks like BOLA attacks can cause several breaches like data exfiltration, full account takeover, etc. The Open Web Application Security Project (OWASP) API Top 10 list and OWAS Web Top 10 list provides guidance on the most critical API and web application vulnerabilities that organizations should try to recognize and remediate. Four of the top five OWASP API Top ten vulnerabilities are related to business logic flaws, and it underscores the fact that business logic vulnerabilities are your top API security risk.

Bad bots, designed to execute malicious attacks on APIs to cause a wide range of data theft and fraud, are another API security threat on the rise. These bad bots should be detected and blocked at all times.

Perimeter solutions may detect and block the most common API threats, but they are not effective against sophisticated API attacks that include different IP addresses, tokens, session IDs, and time periods. Behavioral analytics-based solutions examine API usage, track API consumers, identify normal and abnormal behaviors, and provide actionable business context.

Consider a solution's coverage of the OWASP API Top 10 list, OWASP Web Top 10 list, bad bot management, and behavioral analytics capabilities. These critical elements help the operations and security operations teams provide comprehensive API runtime protection.

Data Exfiltration

As illustrated under the "run time protection" section, there are many ways that APIs can be abused to exfiltrate your sensitive data. Visibility into from which API endpoints and services data are being exfiltrated enables decisive quick action to stop the exfiltrations. Being able to see exactly which sensitive data is being stolen, through which services and API endpoints, by which users, and from what geographies, can aid in prioritization and efficiency in remediation or mitigation. Consider the importance of having these insights available when protecting your data from exfiltration.

In-Line Blocking

API Security solutions should be flexible in how they can be deployed and how they can protect applications. Being able to get started with an out-of-band only solution is a great option to start getting an inventory of all your APIs, and to enable deeper visibility, all with minimal setup overhead and risk to your application. However, **out-of-band** becomes a problem when you want to start blocking bad traffic. If the solution is out-of-band then it needs to block through integrations with external control points, such as API Gateways, WAFs, proxies, etc. Blocking through this mechanism has a few limitations to be aware of.

- The solution can not block the first time that it sees an attack come through. It must first see it, signal the integrated control point, and then assume that the block happened as expected unless a back channel is set up for confirmation.
- Blocking through external control points means increased configuration (with the control points), increased coordination (with the control point owners), and increased maintenance to keep the blocking working.
- Because the detection and blocking steps will be spread across different systems, the method of out-of-band blocking through control points leads to disjointed visibility and audit trails.

Another solution that is good to have as an option is in-line blocking. An API security solution that offers in-line blocking supports blocking directly through its own agents or other in-line software that is part of the single platform (i.e. not 3rd party integrations). This method enables immediate blocking of attacks on detection, ensures blocking happens as expected, and reduces complexity of configuration and maintenance.

Secure API Development

API security testing is vital to prevent vulnerabilities and weaknesses from getting into production, where they can do the most harm, and are the most costly to fix. API security testing aims to ensure APIs behave as designed and don't have API security vulnerabilities in them.



Any API security solution should be focused on the complete API development lifecycle, not just how secure the APIs are in production at runtime. It's important to prevent vulnerabilities by testing for API security before getting to production, as a part of the development and QA cycles. So, consider the value of the ability to support API security testing kicked off from the CI/CD pipeline, the ability to compare the configuration of API endpoints with industry best practices, to run white box testing, and the ability to stop the build pipeline based on API testing results.

TRACEABLE

Noname Security - 70%

Noname Security offers an agentless API security platform intended to help enterprises see and secure their APIs. The company focuses on data collection of APIs and detecting vulnerabilities and misconfigurations before they are exploited. The security platform is an out-of-band solution that doesn't require agents and offers deeper visibility and security than API gateways, load balancers, and WAFs. NoName can initiate blocking of exploit traffic through its connections to third-party control points such as the API gateways, proxies, and load balancers which it is configured to work with.

API Discovery	
Discover all API Endpoints in the system	✓
Auto grouping of discovered APIs into service/application collections	✓
Understand queries, parameters and attributes of the API	✓
Interpret REST, SOAP, gRPC, and GraphQL protocols	✓
Discovery of 3rd party API use and configuration	✓
Identify API changes and versions	✓
Discover and visualize API dependencies	✗
API Security Posture	
Discovery of sensitive data in the APIs	✓
Sensitive data classification (including customized)	✓
Discovery of sensitive data flows	✗
Flagging shadow, zombie, and orphaned endpoints	✓
Ability to create collections and apply policies to them	✓
Ability to manually flag high-risk factors in API endpoints	✓
Automated risk scoring for API Endpoints	✓
Automatically generate and download OpenAPI spec from runtime	✗
OpenAPI spec conformance analysis: runtime vs uploaded	✗
Per API endpoint vulnerability identification	✓
Runtime Protection	
Correlate threat actor (user) activity despite evasion tactics	✗
Automatically track the threat level of each user	✗
Pre-attack threat actor Identification	✗
Detect and block OWASP (Web) Top 10 security events	✗
Detect and block OWASP API Top 10 security events	✓
Detect and block newly-identified CVEs	✓
Identify and block abnormal API behavior (user behavior)	✓

NoName Security (continued)

Runtime Protection (continued)	
Identify and block abnormal API usage rates	✓
Detect and block credential stuffing & Brute forcing (ATO attempts)	✓
Detect and block bad bots use of the APIs	✗
Detect and block application-layer denial of service (DoS) attacks	✗
Enforce protection in heterogeneous environments	✓
Enforce blocking in-line	✗
Enforce blocking cia integrations	✓
Identify APIs and services from which data is being exfiltrated	✗
Secure API Development	
Flag API endpoint configurations not matching industry best practices	✓
Flag API endpoint configurations not matching compan	✓
Pro-active vulnerability detection/probing with a library of known bad payloads	✓
White box security testing	✗
Integration with external defect tracking	✓
Provide API security tests for running in CI/CD pipeline	✓
Can be integrated into CI/CD pipeline to effect pipeline behavior	✓
Provide remediation guidance for developers and operations	✓
API Security Insights	
Analyze the body/payloads of requests and responses	✓
Detect suspicious client requests based on IP reputation	✓
Identify geo-location of API calls to help with API risk assessments	✓
API Performance metrics, call and error patterns	✓
Correlate and end-to-end connect all application API transactions	✗
Deep API transaction context for API incident response and threat hunting	✗
Share data with SIEM, SOAR, and ITSM systems	✓
Architecture & Deployment	
AI/ML based security and anomaly analysis	✓
Agentless (Mirroring, Out-of-band)	✓
Agentless (Edge - proxies, gateways, mesh)	✓
Agent-based (language-specific, In-line)	✗
Platform backend offered as SaaS offering	✓
Backend deployment on customer prem/cloud (self managed, air gapped)	✓

Some things to investigate when considering NoName Security

API Discovery & Visualisation of API Dependencies

Maintaining accurate, up-to-date API inventory is critical to understanding potential risk and exposure. An outdated inventory results in widening the attack surface and creating more blind spots for your security teams. A continuous API discovery helps to identify and catalog all API endpoints, functions, and API parameters etc. Automated API discovery, API inventory, and classification of all APIs used by your applications, including shadow APIs, make it easy for you to be aware of changes and evolving risks.

Ideally, every vendor should have API dependency mapping and related visualizations as part of their API discovery capabilities. This capability should shed light on the data flow between services across application environments and provide a live view of all API requests. API dependency visualization provides actionable visibility for developers and security operation teams in Root Cause Analysis (RCA) and faster remediation.

Automated API Endpoint Risk Scoring

When we talk about an API what we are really talking about is the collection of endpoints that comprise the API. A single API can have tens or even hundreds of API endpoints, each one presenting a potential attack surface. And each endpoint will have its own characteristics which factor into how risky it is for it to cause a breach. Given this, consider how incredibly valuable it is to not just have an inventory of all your APIs, but also some way to prioritize them according to how much risk they pose to your application security. An overall API security posture rating for the whole set of APIs which rolls up a score based the total number of vulnerabilities will not be granular enough to focus team efforts. To quickly identify the top risky API endpoints from the potentially hundreds or thousands that will likely be in your inventory it's important to have a per endpoint risk score.

Additionally, the factors that should be included in the risk score analysis will constantly be changing across the set of API endpoints. This means that the risk score really needs to be automatically and continuously calculated to give up to date assessments. When looking at API endpoint risk scoring solutions, make sure that the scores can be calculated automatically, as manual risk tracking will quickly become stale.

Sensitive Data Flow and Classification

Maintaining an API catalog that classifies sensitive data, like PII, PCI, PHI, PCI-DSS, etc is essential in quickly identifying and mitigating data breaches. You should look for a solution that has the ability to identify which services, API endpoints, and users are using your sensitive data. Knowing how your sensitive data flows across your services and APIs enables you to identify insecure or vulnerable APIs that could lead to devastating data breaches.

Runtime Protection

Business Logic attacks like BOLA attacks can cause several breaches like data exfiltration, full account takeover, etc. The Open Web Application Security Project (OWASP) API Top 10 list and OWAS Web Top 10 list provides guidance on the most critical API and web application vulnerabilities that organizations should try to recognize and remediate. Four of the top five OWASP API Top ten vulnerabilities are related to business logic flaws, and it underscores the fact that business logic vulnerabilities are your top API security risk.

Bad bots, designed to execute malicious attacks on APIs to cause a wide range of data theft and fraud, are another API security threat on the rise. These bad bots should be detected and blocked at all times.

Perimeter solutions may detect and block the most common API threats, but they are not effective against sophisticated API attacks that include different IP addresses, tokens, session IDs, and time periods. Behavioral analytics-based solutions examine API usage, track API consumers, identify normal and abnormal behaviors, and provide actionable business context.

Consider a solution's coverage of the OWASP API Top 10 list, OWASP Web Top 10 list, bad bot management, and behavioral analytics capabilities. These critical elements help the operations and security operations teams provide comprehensive API runtime protection.

Data Exfiltration

As illustrated under the "run time protection" section, there are many ways that APIs can be abused to exfiltrate your sensitive data. Visibility into from which API endpoints and services data are being exfiltrated enables decisive quick action to stop the exfiltrations. Being able to see exactly which sensitive data is being stolen, through which services and API endpoints, by which users, and from what geographies, can aid in prioritization and efficiency in remediation or mitigation. Consider the importance of having these insights available when protecting your data from exfiltration.

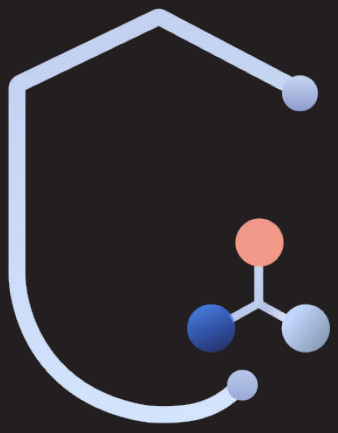
In-Line Blocking

API Security solutions should be flexible in how they can be deployed and how they can protect applications. Being able to get started with an out-of-band only solution is a great option to start getting an inventory of all your APIs, and to enable deeper visibility, all with minimal setup overhead and risk to your application. However, **out-of-band** becomes a problem when you want to start blocking bad traffic. If the solution is out-of-band then it needs to block through integrations with external control points, such as API Gateways, WAFs, proxies, etc. Blocking through this mechanism has a few limitations to be aware of.

- The solution can not block the first time that it sees an attack come through. It must first see it, signal the integrated control point, and then assume that the block happened as expected unless a back channel is set up for confirmation.audit trails.

- Blocking through external control points means increased configuration (with the control points), increased coordination (with the control point owners), and increased maintenance to keep the blocking working.
- Because the detection and blocking steps will be spread across different systems, the method of out-of-band blocking through control points leads to disjointed visibility and audit trails.

Another solution that is good to have as an option is in-line blocking. An API security solution that offers in-line blocking supports blocking directly through its own agents or other in-line software that is part of the single platform (i.e. not 3rd party integrations). This method enables immediate blocking of attacks on detection, ensures blocking happens as expected, and reduces complexity of configuration and maintenance.



TRACEABLE

Traceable AI - 96%

Traceable identifies all of your APIs, evaluates your API risk posture, stops API attacks that lead to incidents such as data exfiltration, and provides analytics for threat hunting and forensic research. With Traceable, you can confidently discover, manage and secure all of your APIs, quickly deploy, and easily scale to meet the ongoing needs of your organization.

Traceable can deploy agentless out-of-band through various forms of traffic mirroring, agentless edge through plugins on edge infrastructure such as API gateways, load balancers, proxies, and meshes, and even in-app through language agents to be closer to the code for enhanced API call level troubleshooting and analytics.

API Discovery	
Discover all API Endpoints in the system	✓
Auto grouping of discovered APIs into service/application collections	✓
Understand queries, parameters and attributes of the API	✓
Interpret REST, SOAP, gRPC, and GraphQL protocols	✓
Discovery of 3rd party API use and configuration	✓
Identify API changes and versions	✓
Discover and visualize API dependencies	✓
API Security Posture	
Discovery of sensitive data in the APIs	✓
Sensitive data classification (including customized)	✓
Discovery of sensitive data flows	✓
Flagging shadow, zombie, and orphaned endpoints	✓
Ability to create collections and apply policies to them	✓
Ability to manually flag high-risk factors in API endpoints	✓
Automated risk scoring for API Endpoints	✓
Automatically generate and download OpenAPI spec from runtime	✓
OpenAPI spec conformance analysis: runtime vs uploaded	✓
Per API endpoint vulnerability identification	✓
Runtime Protection	
Correlate threat actor (user) activity despite evasion tactics	✓
Automatically track the threat level of each user	✓
Pre-attack threat actor Identification	✓
Detect and block OWASP (Web) Top 10 security events	✓
Detect and block OWASP API Top 10 security events	✓
Detect and block newly-identified CVEs	✓

Traceable AI (continued)

Runtime Protection (continued)	
Identify and block abnormal API behavior (user behavior)	✓
Identify and block abnormal API usage rates	✓
Detect and block credential stuffing & Brute forcing (ATO attempts)	✓
Detect and block bad bots use of the APIs	✓
Detect and block application-layer denial of service (DoS) attacks	✓
Enforce protection in heterogeneous environments	✓
Enforce blocking in-line	✓
Enforce blocking cia integrations	✓
Identify APIs and services from which data is being exfiltrated	✓
Secure API Development	
Flag API endpoint configurations not matching industry best practices	✗
Flag API endpoint configurations not matching compan	✗
Pro-active vulnerability detection/probing with a library of known bad payloads	✓
White box security testing	✓
Integration with external defect tracking	✓
Provide API security tests for running in CI/CD pipeline	✓
Can be integrated into CI/CD pipeline to effect pipeline behavior	✓
Provide remediation guidance for developers and operations	✓
API Security Insights	
Analyze the body/payloads of requests and responses	✓
Detect suspicious client requests based on IP reputation	✓
Identify geo-location of API calls to help with API risk assessments	✓
API Performance metrics, call and error patterns	✓
Correlate and end-to-end connect all application API transactions	✓
Deep API transaction context for API incident response and threat hunting	✓
Share data with SIEM, SOAR, and ITSM systems	✓
Architecture & Deployment	
AI/ML based security and anomaly analysis	✓
Agentless (Mirroring, Out-of-band)	✓
Agentless (Edge - proxies, gateways, mesh)	✓
Agent-based (language-specific, In-line)	✓
Platform backend offered as SaaS offering	✓
Backend deployment on customer prem/cloud (self managed, air gapped)	✓

Some things to investigate when considering Traceable AI

API Discovery & Visualisation of API Dependencies

A continuous API discovery process helps to identify and catalog all API endpoints, functions, API parameters, and more. Ideally, every vendor should have API dependency mapping and related visualizations as part of their API discovery capabilities. This capability sheds light on the data flow between services, across application environments, and provides a live view of all API requests. API dependency visualization provides actionable visibility for developers and security operation teams to quickly perform Root Cause Analysis (RCA) and remediation.

Automated API Endpoint Risk Scoring

Take a look at any list of API endpoints in Traceable and you'll see that you can prioritize your efforts using the API endpoint risk scoring. Note also how it rolls up to services and how you can dig deeper into any score to truly understand the details of how the score was generated. And if the scoring system doesn't align with your organization's sense of risk, you can tune the scoring mechanism to make it fit.

Runtime Protection

When it comes to effective API security protection Traceable has you covered with a broad range of capabilities that are required to stay secure.

For runtime protection Traceable offers the ability to detect and block attacks on both known and unknown API vulnerabilities, such as the OWASP API Top 10 vulnerabilities, the OWASP Web Top 10 vulnerabilities, other business logic abuse attacks, and zero days. Traceable also protects your APIs by detecting and blocking bad bots, API abuse, and API fraud. Finally, identifying live and histrical data exfiltration enables you to stop remediate or mitigate.

Traceable enables you to stay on top of detecting and protecting by combining big data from distributed tracing with machine learning to bring you only the most pertinent information. For example, the Threat actors screen highlights the user of your applications who have exhibited the most malicious behavior. The APIs Under Threat gives you a live view of APIs currently being attacked, and the Threat Activity dashboard gives you a summary your overall API security posture, with the ability to get to the details in one click.

Data Exfiltration

Take a look at the Data Protection view to see all the details about data that is being exfiltrated from your applications. You can see a historical view to find trends, and a live view, to know where you need to take action right away. Take a look at the provided data about the data types and classifications, which services and API endpoints they got exfiltrated through, and which users stole the data, as well as what else they got. Once you've identified the user you want to stop, go to the threat actors' screen and block them from all actions across all your apps.

Secure API Development

API security testing is vital to prevent vulnerabilities and weaknesses from getting into production, where they can do the most harm, and are the most costly to fix. API security testing aims to ensure APIs behave as designed and don't have API security vulnerabilities in them.

Any API security solution should be focused on the complete API development lifecycle, not just how secure the APIs are in production at runtime. It's important to prevent vulnerabilities by testing for API security before getting to production, as a part of the development and QA cycles. So, consider the value of the ability to support API security testing kicked off from the CI/CD pipeline, the ability to compare the configuration of API endpoints with industry best practices, to run white box testing, and the ability to stop the build pipeline based on API testing results.

Security Data Lake for Threat Hunting

Explore more about Traceable's data lake and how it enables threat hunting, post-forensic analysis, and tracking of sensitive data flows across API-driven applications. Do some queries and you'll start seeing how you can use the data lake to detect and protect against business logic exploits, API abuse, fraud, find collateral damage, and shorten MTTR.



TRACEABLE

API Security Solution Comparison Matrix

	SALT	noname	TRACEABLE
API Discovery			
Discover all API Endpoints in the system	✓	✓	✓
Auto grouping of discovered APIs into service/application collections	✗	✓	✓
Understand queries, parameters and attributes of the API	✓	✓	✓
Interpret REST, SOAP, gRPC, and GraphQL protocols	✓	✓	✓
Discovery of 3rd party API use and configuration	✓	✓	✓
Identify API changes and versions	✓	✓	✓
Discover and visualize API dependencies	✗	✗	✓
API Security Posture			
Discovery of sensitive data in the APIs	✓	✓	✓
Sensitive data classification (including customized)	✓	✓	✓
Discovery of sensitive data flows	✗	✗	✓
Flagging shadow, zombie, and orphaned endpoints	✓	✓	✓
Ability to create collections and apply policies to them	✗	✓	✓
Ability to manually flag high-risk factors in API endpoints	✗	✓	✓
Automated risk scoring for API Endpoints	✗	✓	✓
Automatically generate and download OpenAPI spec from runtime	✓	✗	✓
OpenAPI spec conformance analysis: runtime vs uploaded	✓	✗	✓
Per API endpoint vulnerability identification	✓	✓	✓
Runtime Protection			
Correlate threat actor (user) activity despite evasion tactics	✗	✗	✓
Automatically track the threat level of each user	✗	✗	✓
Pre-attack threat actor Identification	✓	✗	✓
Detect and block OWASP (Web) Top 10 security events	✗	✗	✓
Detect and block OWASP API Top 10 security events	✓	✓	✓
Detect and block newly-identified CVEs	✓	✓	✓
Identify and block abnormal API behavior (user behavior)	✓	✓	✓
Identify and block abnormal API usage rates	✓	✓	✓
Detect and block credential stuffing & Brute forcing (ATO attempts)	✓	✓	✓
Detect and block bad bots use of the APIs	✗	✗	✓
Detect and block application-layer denial of service (DoS) attacks	✓	✗	✓
Enforce protection in heterogeneous environments	✓	✓	✓
Enforce blocking in-line	✗	✗	✓

API Security Solution Comparison Matrix (continued)

	SALT	noname	TRACEABLE
Runtime Protection (continued)			
Enforce blocking cia integrations	✓	✓	✓
Identify APIs and services from which data is being exfiltrated	✗	✗	✓
Secure API Development			
Flag API endpoint configurations not matching industry best practices	✗	✓	✗
Flag API endpoint configurations not matching compan	✓	✓	✗
Pro-active vulnerability detection/probing with a library of known bad payloads	✗	✓	✓
White box security testing	✗	✗	✓
Integration with external defect tracking	✓	✓	✓
Provide API security tests for running in CI/CD pipeline	✗	✓	✓
Can be integrated into CI/CD pipeline to effect pipeline behavior	✗	✓	✓
Provide remediation guidance for developers and operations	✓	✓	✓
API Security Insights			
Analyze the body/payloads of requests and responses	✓	✓	✓
Detect suspicious client requests based on IP reputation	✓	✓	✓
Identify geo-location of API calls to help with API risk assessments	✓	✓	✓
API Performance metrics, call and error patterns	✓	✓	✓
Correlate and end-to-end connect all application API transactions	✗	✗	✓
Deep API transaction context for API incident response and threat hunting	✗	✗	✓
Share data with SIEM, SOAR, and ITSM systems	✓	✓	✓
Architecture & Deployment			
AI/ML based security and anomaly analysis	✓	✓	✓
Agentless (Mirroring, Out-of-band)	✓	✓	✓
Agentless (Edge - proxies, gateways, mesh)	✓	✓	✓
Agent-based (language-specific, In-line)	✗	✗	✓
Platform backend offered as SaaS offering	✓	✓	✓
Backend deployment on customer prem/cloud (self managed, air gapped)	✗	✓	✓
	60%	70%	96%

A Note About This Guide

This analysis and comparison are based on research of public-facing documentation and content and are intended to educate and inform the market about how different solutions address API security capabilities. We welcome feedback to make this evaluation more accurate. If you see any errors or ommissions please connect with us and we'll be happy to update the content.

For this new version of the guide, we increased the depth of the capabilities analysis, and focused in on a few top vendors in the API Security space. Over time we will do the analysis of others and add them to this guide. In the meantime, you can see the original assessments in the appendix.

About us

Traceable is the industry's leading API security platform that identifies APIs, evaluates API risk posture, stops API attacks, and provides deep analytics for threat hunting and forensic research. With visual depictions of API paths at the core of its technology, its platform applies the power of distributed tracing and machine learning models for API security across the entire development lifecycle.

Visual depictions provide insight into user and API behaviors to understand anomalies and block API attacks, enabling organizations to be more secure and resilient.

Learn more at traceable.ai.

www.traceable.ai



TRACEABLE_

Intelligent API Security at Enterprise Scale

Doc Ver: 2022-10-11-01

Appendix

API Security Market Overview

(predecessor to current guide)

Modern applications, composed of microservices and cloud-native architectures, enable rapid innovation and the creation of business value. Enabling collaboration and partnership in the market, APIs are the cement in the foundation of modern applications. Managing API security risks is a rapidly growing challenge facing engineering, IT, and security leaders. This comprehensive comparison guide is based on a collection of 14 API Security Tool Requirements, organized into 5 groups. Specifically, an API security tool must be able to account for the following overarching security requirements:

API Security Requirements Overview

API Discovery and Risk Management - Find, catalog, and analyze ALL APIs in an application

- API Disovery
- API Risk Management
- API Change Dectection
- Usage Analysis
- 3rd Party API Risk

Detection and Blocking of Attacks - Detect and thwart adversarial attacks

- OWASP Top 10 Attacks - Legacy
- OWASP API Top 10 Attacks
- DDoS Protection

User Behavior Attacks - Detect and mitigate fraud and abuse of APIs

- User Identification & Behavior Analytics
- Bot Mitigation
- Fraud Detection

Data Flow Analytics - Leverage data to enable threat hunting and analytics

- Sensitive Data Flow
- Analytics & Threat Hunting

Deployment Options - Deploy and detect both:

- Inline / Agent-based
- Out-of-Band / Agentless

The API security tool landscape consists of many different entries, from traditional firewall/edge-based protection solutions to solutions that leverage modern techniques like distributed tracing and observability to see inside of API traffic to detect potential anomalies and attacks.

API Security Tool Requirements

API Discovery and Risk Management

API Discovery

Ensures that you always have an up-to-date inventory of your organization's APIs. Continuously discovers and inventories all APIs, including shadow APIs of an organization. Provides change notification when API has been added, modified, or deprecated.

API Risk Monitoring

Continuously updated endpoint risk scoring based on the likelihood and impact of a cyberattack. Example risk-score criteria are: external vs internal API, unauthenticated, has a global user-base, and handles sensitive data.

API Change Detection

The ability to detect and flag changes in API specifications, configuration, and/or parameter details so that unexpected and potentially insecure changes (malicious or not) can be caught and validated before problems arise.

Usage Analysis

Helps to track and understand usage patterns of APIs, monitor performance of APIs, diagnose issues between APIs and applications.

3rd-Party API Risk

Discover 3rd party APIs that integrate with your application that might pose an unknown risk to your organization.

Detecting and Blocking Attacks

OWASP Top 10 Attacks - Legacy

Detection and blocking of the OWASP Top 10 vulnerabilities, which provide guidance to developers and security professionals on the most critical vulnerabilities that are commonly found in web applications.

OWASP API Top 10 Attacks

Detection and blocking of the OWASP API Top 10 vulnerabilities. Protects against BOLA, mass assignment, and business logic flaws.

DDoS Protection

DDoS (distributed denial of service) protection foils malicious traffic coming from multiple network points before reaching their destination, minimizing the impact of the attack while ensuring legitimate traffic flow.

Detecting and Blocking Attacks

User Identification & Behavior Analytics

Uses advanced user identification and analytics technologies, including machine learning and deep learning, to discover abnormal and risky behavior by users, machines, and other entities interacting with your applications.

Bot Mitigation

Bot mitigation is the process of minimizing risk to applications, websites, APIs, etc. from malicious bot traffic. Bot mitigation solutions use different techniques to identify, manage and block bad bots while allowing legitimate bots to operate.

Fraud Detection

Fraud detection protects customer and enterprise information, assets, accounts, and transactions through the real-time, near-real-time, or batch analysis of activities by users and other defined entities (such as kiosks). It uses background server-based processes that examine users' and other defined entities' access and behavior patterns and typically compares this information to a profile of what's expected.

Data Flow Analytics

Sensitive Data Flow

Prevent sensitive data exposure. Identify API endpoints that handle sensitive data. See meta-data details of all data used by all endpoints. Identify external facing and internal APIs handling sensitive data. Identify APIs endpoints without authentication.

Analytics & Threat Hunting

An explorable data lake of all transaction details which can be filtered, sorted, and searched to find meaningful data, discover trends, and gain insights. Explorability of this data collection enables threat hunting and forensics.

Deployment Options

Inline / Agent-based

A deployment option that uses an in-app agent which sits in line with the application. In-app agents are typically libraries that can be linked in at runtime without code alteration. Typically inline/agent-based deployments can provide deeper system-level insights for better overall visibility and control points for more direct application protection.

Out-of-Band/Agentless

An out-of-band agentless deployment means that functionality is achieved without requiring any application code changes and that there is no agent in the path of the application communications. This is typically achieved either through traffic mirroring or from log and metrics collection from infrastructure devices. Out-of-band/agentless typically do not provide as deep a set of application data as agent-based data collection.

Signal Sciences - 32%

Signal Sciences offers a WAF that can protect your web application based on security signatures.

Considerations

Just Web Protection

Cybercriminals have expanded their attack campaigns to both web and API applications, looking for an easy way to breach your security defenses and steal your sensitive data. Without a solid defense against web and API attacks, you end up with a hole in your security protection, allowing cybercriminals to gain an easy foothold in your organization.

Real API Security

APIs expose business logic, and attackers often exploit your business logic to abuse your APIs. Understanding API context and transaction/data flows are crucial to detecting and defending against business logic attacks. You need a solution that understands an application's business logic. Purpose-built to detect and block business logic attacks by analyzing transactions and data flow – helping to thwart sophisticated API attacks that target your mission-critical application's sensitive data. Suggest evaluating how to block business logic attacks such as BOLA.

API Security Requirements	Signal Sciences (32%)
API Discovery and Risk Management	
APIs Discovery	X
API Risk Monitoring	X
API Change Detection	X
Usage Analysis	X
3rd party API Risk	X
Detection and Blocking of Attacks	
OWASP Top 10 attacks - WAF	✓
OWASP API Top 10 attacks	Partial
DDoS Protection	Partial
User Behavior Attacks	
User Identification & Behavior Analytics	X
Bot Mitigation	✓
Fraud Detection	Partial
Data Flow Analytics	
Sensitive Data Flow	X
Security Data Lake For Analytics & Threat hunting	X
Deployment	
Inline / Agent-based	✓
Out-of-Band/Agentless	X

API Parameter Definition

The problem with OpenAPI parameter files right from the start was that they were difficult to update and maintain, pulling the developer away from the serious work of developing new software features. If a developer doesn't update that API parameter file, it can leave the door wide open for a cybercriminal to target and exploit your API application.

Sensitive Data Tracking

Maintaining an API catalog that highlights sensitive data, like PII, PCI, etc exposure is a critical step in mitigating data breaches. Consider evaluating how Signal Sciences will detect and prevent unauthorized sensitive data from flowing through your APIs.

Security Data Lake

Historical data about attempted API attacks is a crucial need for security teams to improve their security posture over time. You need a solution that is built on a security data lake that enables EDR-like capabilities that enterprise security teams have been using for years. Customers will be able to perform threat hunting, post-forensic analysis and track sensitive data flows across their API-driven applications.

42Crunch - 21%

42Crunch provides a platform that enables an automated set of tools that help to secure APIs throughout the software development cycle. Built around a positive API security model based on the Open API/Swagger file, 42Crunch can help automate security checks throughout your CI/CD pipelines. Throughout the process, it can execute detailed security checks, providing security scores and remediation advice to developers. This finalized contract is used to provide real-time security enforcement with their API firewall.

API Security Requirements	42Crunch (21%)
API Discovery and Risk Management	
APIs Discovery	X
API Risk Monitoring	✓
API Change Detection	✓
Usage Analysis	X
3rd party API Risk	X
Detection and Blocking of Attacks	
OWASP Top 10 attacks - WAF	X
OWASP API Top 10 attacks	✓
DDoS Protection	X
User Behavior Attacks	
User Identification & Behavior Analytics	X
Bot Mitigation	X
Fraud Detection	X
Data Flow Analytics	
Sensitive Data Flow	X
Security Data Lake For Analytics & Threat hunting	X
Deployment	
Inline / Agent-based	X
Out-of-Band/Agentless	X

Considerations

Open API File-Based Protection

The problem with OpenAPI parameter files right from the start was that they were difficult to update and maintain, pulling the developer away from the serious work of developing new software features. If a developer doesn't update that API parameter file, it can leave the door wide open for a cybercriminal to target and exploit your API application. Traceable is able to automatically discover and update all API parameter changes, without the need to maintain an OpenAPI file, ensuring that your API Security is automated and up-to-date.

Business Logic Understanding

APIs expose business logic, and attackers often exploit your business logic to abuse your APIs. Understanding API context and transaction/data flows are crucial to detecting and defending against business logic attacks. Suggest exploring how 42Crunch can detect and block business logic attacks.

Continued on next page...

Sensitive Data Tracking

Maintaining an API catalog that highlights sensitive data, like PII, PCI, etc exposure is a critical step in mitigating data breaches. You need a solution that has the ability to pinpoint your sensitive data and identify and visualize each API flow across your applications, allowing you to identify insecure or vulnerable APIs that could lead to a devastating data breach.

Security Data Lake

Historical data about attempted API attacks is a crucial need for security teams to improve their security posture over time. You need a solution that is built on a security data lake that enables EDR-like capabilities that enterprise security teams have been using for years. Customers will be able to perform threat hunting, post-forensic analysis and track sensitive data flows across their API-driven applications.

Neosec - 68%

Neosec is an intelligent application security platform based on data and behavioral analytics. Neosec is the XDR equivalent for API security.

Considerations

Data Collection

Neosec collects data from existing API activity happening around the application itself, without deploying sensors of sidecars. Is Neosec working with all the data? How does it understand internal application logic without deriving it from what it see's externally?

Real-Time Enforcement

Neosec blocking capability is through integrations with 3rd party vendors such as API gateways and proxies, which can delay enforcement by seconds.

Web Protection & API Protection

Neosec focuses on API security only, not web application protection too.

Cybercriminals often target both web and API applications of an organization, looking for an easy unprotected way to access sensitive data. Not having an integrated and complete security solution that covers both web and API security is an invitation to cybercriminals to target your organization.

API Security Requirements	Neosec (68%)
API Discovery and Risk Management	
APIs Discovery	✓
API Risk Monitoring	✓
API Change Detection	X
Usage Analysis	✓
3rd party API Risk	✓
Detection and Blocking of Attacks	
OWASP Top 10 attacks - WAF	X
OWASP API Top 10 attacks	✓
DDoS Protection	X
User Behavior Attacks	
User Identification & Behavior Analytics	✓
Bot Mitigation	Partial
Fraud Detection	✓
Data Flow Analytics	
Sensitive Data Flow	X
Security Data Lake For Analytics & Threat hunting	✓
Deployment	
Inline / Agent-based	X
Out-of-Band/Agentless	✓

Cequence - 57%

Cequence Security was founded in 2015 as a bot mitigation and fraud prevention company. More recently, Cequence repositioned itself as an API Security vendor with the introduction of API Sentinel. However, API Sentinel offers basic API discovery and visibility features that are common across most API Security vendors. Beyond that, it doesn't offer any focused API Security features that are required to protect mission-critical applications. Despite the new API Sentinel product introduction, Cequence is still primarily a bot mitigation company with basic API Security coverage.

Considerations

Understanding of Business Logic

APIs expose business logic, and attackers often exploit your business logic to abuse your APIs. Understanding API context and transaction/data flows are crucial to detecting and defending against business logic attacks.

API Security Data Lake

Historical data about attempted API attacks is a crucial need for security teams to improve their security posture over time. You need a solution that is built on a security data lake that enables EDR-like capabilities that enterprise security teams have been using for years. Customers need the ability to perform threat hunting, post-forensic analysis and track sensitive data flows across their API-driven applications.

API Security Requirements	Cequence (57%)
API Discovery and Risk Management	
APIs Discovery	✓
API Risk Monitoring	✓
API Change Detection	X
Usage Analysis	✓
3rd party API Risk	X
Detection and Blocking of Attacks	
OWASP Top 10 attacks – WAF	✓
OWASP API Top 10 attacks	✓
DDoS Protection	X
User Behavior Attacks	
User Identification & Behavior Analytics	X
Bot Mitigation	✓
Fraud Detection	✓
Data Flow Analytics	
Sensitive Data Flow	X
Security Data Lake For Analytics & Threat hunting	X
Deployment	
Inline / Agent-based	X
Out-of-Band/Agentless	✓

Sensitive Data Tracking

Maintaining an API catalog that highlights sensitive data, like PII, PCI, etc exposure is a critical step in mitigating data breaches. You need a solution that has the ability to pinpoint your sensitive data and identify and visualize each API flow across your applications, allowing you to identify insecure or vulnerable APIs that could lead to a devastating data breach.

Data Theorem - 36%

Data Theorem is a provider of application security analysis software. Data Theorem can discover and inventory all your APIs. Data Theorem's analyzer engine continuously scans mobile and web applications in search of security flaws and data privacy gaps. IT can discover and inventory your APIs and discover potential API vulnerabilities. By integrating with your CI/CD pipeline, it can remediate potential security issues such as authentication, authorization, encryption, etc.

Considerations

Real-Time Protection

API attacks are fast and hard to detect because they often look like regular business traffic. Organizations need deployment options that takes minutes to set up. This includes an in-app agent option for real-time protection, blocking threats as they come, and an agentless option that can be deployed outside the application depending on your requirements.

Security Data Lake

Historical data about attempted API attacks is a crucial need for security teams to improve their security posture over time. You need a solution that is built on a security data lake that enables EDR-like capabilities that enterprise security teams have been using for years. Customers need the ability to perform threat hunting, post-forensic analysis and track sensitive data flows across their API-driven applications.

API Security Requirements	Data Theorem (36%)
API Discovery and Risk Management	
APIs Discovery	✓
API Risk Monitoring	X
API Change Detection	✓
Usage Analysis	X
3rd party API Risk	X
Detection and Blocking of Attacks	
OWASP Top 10 attacks - WAF	✓
OWASP API Top 10 attacks	✓
DDoS Protection	X
User Behavior Attacks	
User Identification & Behavior Analytics	X
Bot Mitigation	X
Fraud Detection	X
Data Flow Analytics	
Sensitive Data Flow	X
Security Data Lake For Analytics & Threat hunting	X
Deployment	
Inline / Agent-based	X
Out-of-Band/Agentless	✓

Business Logic Understanding

APIs expose business logic, and attackers often exploit your business logic to abuse your APIs. Understanding API context and transaction/data flows are crucial to detecting and defending against business logic attacks.

Wib - 57%

Wib is a relatively new vendor in the API Security landscape. The company provides API Security across the entire API software development lifecycle like many other vendors in the industry. Wib, which claims to protect APIs through the entire API software development lifecycle, does not provide rich business context needed to identify vulnerabilities and prevent API attacks in real time. Wib is able to meet just over half of the API security requirements delivering 8 out 14, meeting the basic needs of some organizations.

Considerations

Real-Time Protection

API attacks are fast and hard to detect because they often look like regular business traffic. Organizations need deployment options that takes minutes to set up. This includes an in-app agent option for real-time protection, blocking threats as they come, and an agentless option that can be deployed outside the application depending on your requirements.

Security Data Lake

Historical data about attempted API attacks is a crucial need for security teams to improve their security posture over time. You need a solution that is built on a security data lake that enables EDR-like capabilities that enterprise security teams have been using for years. Customers need the ability to perform threat hunting, post-forensic analysis and track sensitive data flows across their API-driven applications.

API Security Requirements	Wib (57%)
API Discovery and Risk Management	
APIs Discovery	✓
API Risk Monitoring	✓
API Change Detection	✓
Usage Analysis	Partial
3rd party API Risk	✓
Detection and Blocking of Attacks	
OWASP Top 10 attacks - WAF	X
OWASP API Top 10 attacks	✓
DDoS Protection	X
User Behavior Attacks	
User Identification & Behavior Analytics	✓
Bot Mitigation	X
Fraud Detection	Partial
Data Flow Analytics	
Sensitive Data Flow	X
Security Data Lake For Analytics & Threat hunting	X
Deployment	
Inline / Agent-based	X
Out-of-Band/Agentless	✓

Web Protection

Cybercriminals have expanded their attack campaigns to both Web and API applications, looking for an easy way to breach your security defenses and steal your sensitive data. Without a solid defense against web and API attacks, you end up with a hole in your security protection, allowing cybercriminals to gain an easy foothold in your organization.

Traceable AI - 96%

Traceable AI collects API traffic across the entire application landscape and uses context-based behavioral analytics AI engine to discover APIs and what data they expose, block known and unknown attacks, and provide threat analytics and forensics.

Traceable AI uses both agentless deployment options, including out-of-band traffic mirroring and language agents to be closer to the code for enhanced API call level troubleshooting and analytics. Based on this approach Traceable is able to address almost all of the API Security Requirements, delivering 13 ½ out of 14 requirements.

API Security Requirements	Traceable AI (96%)
API Discovery and Risk Management	
APIs Discovery	✓
API Risk Monitoring	✓
API Change Detection	✓
Usage Analysis	✓
3rd party API Risk	✓
Detection and Blocking of Attacks	
OWASP Top 10 attacks - WAF	✓
OWASP API Top 10 attacks	✓
DDoS Protection	X
User Behavior Attacks	
User Identification & Behavior Analytics	✓
Bot Mitigation	✓
Fraud Detection	Partial
Data Flow Analytics	
Sensitive Data Flow	✓
Security Data Lake For Analytics & Threat hunting	✓
Deployment	
Inline / Agent-based	✓
Out-of-Band/Agentless	✓

Considerations

Complete API Catalog

Due to close integration into the application, Traceable AI is able to detect and maintain a complete and accurate API Catalog.

Real-Time Protection

Traceable is able to deliver real-time in-app blocking and agentless deployment options.

Understanding of Business Logic

Traceable AI is able to detect and block sophisticated API attacks that focus on Business logic exploits that can lead to sensitive data exposure.

Security Data Lake for Threat Hunting

Traceable's data lake enables EDR-like capabilities that enterprise security teams can perform threat hunting, post-forensic analysis and track sensitive data flows across their API-driven applications.

Continued on next page...

Sensitive Data Tracking

Traceable has the ability to pinpoint sensitive data and identify and visualize each API flow across applications, allowing teams to identify insecure or vulnerable APIs that could lead to a devastating data breach.

Learn more about how Traceable AI provides complete API Security coverage.

The API Security Market Overview

API Security Requirements	Signal Sciences (32%)	Noname (43%)	Salt Security (50%)	42Crunch (21%)	CloudFlare (61%)	Neosec (68%)	Cequence (57%)	Data Theorem (36%)	Wib (57%)	Traceable AI (96%)
API Discovery and Risk Management										
APIs Discovery	x	✓	✓	x	✓	✓	✓	✓	✓	✓
API Risk Monitoring	x	✓	✓	✓	✓	✓	✓	x	✓	✓
API Change Detection	x	✓	x	✓	x	x	x	✓	✓	✓
Usage Analysis	x	x	✓	x	✓	✓	✓	x	Partial	✓
3rd party API Risk	x	x	✓	x	x	✓	x	x	✓	✓
Detection and Blocking of Attacks										
OWASP Top 10 attacks - WAF	✓	Partial	✓	x	✓	x	✓	✓	x	✓
OWASP API Top 10 attacks	Partial	✓	✓	✓	✓	✓	✓	✓	✓	✓
DDoS Protection	Partial	x	x	x	✓	x	x	x	x	x
User Behavior Attacks										
User Identification & Behavior Analytics	x	x	x	x	x	✓	x	x	✓	✓
Bot Mitigation	✓	x	x	x	✓	Partial	✓	x	x	✓
Fraud Detection	Partial	Partial	x	x	Partial	✓	✓	x	Partial	Partial
Data Flow Analytics										
Sensitive Data Flow	x	x	x	x	x	x	x	x	x	✓
Security Data Lake For Analytics & Threat hunting	x	x	x	x	x	✓	x	x	x	✓
Deployment										
Inline / Agent-based	✓	x	x	x	x	x	x	x	x	✓
Out-of-Band/Agentless	x	✓	✓	x	✓	✓	✓	✓	✓	✓

The sections below, provide a deeper dive into each of the above nine solutions based on the fourteen API Security Requirements.

- Signal Sciences - 32%
- Noname - 45%
- Salt Security - 50%
- 42Crunch - 21%
- Neosec - 68%
- Cequence - 57%
- Data Theorem - 36%
- Wib - 57%
- Traceable AI - 96%

Note: The % score is based on the number of API Security requirements the tool meets divided by the number of API Security requirements (14). Partial = ½ credit.