

# CloudVector Enterprise Edition: Deep API Visibility is the Foundation of API Data Protection



## YOU CANNOT PROTECT WHAT YOU DO NOT KNOW EXISTS

Visibility is critical to security because the ability for APIs to transport sensitive information is inherently risky. It is also tricky to define visibility. Certainly, it is important to have a comprehensive understanding of the entire enterprise environment, but it is even more important to understand how data can move through that environment. It is good to be able to identify the hundreds of APIs in an enterprise environment, but it is even better to be able to focus on a dozen that matter most – those with access to sensitive data or vulnerable to exploits. Visibility is not just seeing APIs and monitoring data flows, it is understanding their risks.

Digital transformation has accelerated the speed of business. Security teams need a solution that can keep pace with rapid DevOps. They need a solution that can provide visibility into monitoring the blur of data moving between APIs. For true API security, they need to go deep inside the data. They need CloudVector Enterprise Edition.

## CLOUDVECTOR ENTERPRISE EDITION: UNPARALLELED VISIBILITY INTO DATA IN TRANSIT

CloudVector Enterprise Edition leverages its unique micro sensor architecture to automatically and continuously discover and monitor all APIs in real time. Its deep API inspection provides the most comprehensive insights into API behavior. CloudVector Enterprise Edition delivers superior API visibility across multiple dimensions. And best of all, CloudVector can be deployed with zero impact to developers and their applications, so that security doesn't become a hindrance to DevOps.

## API VISIBILITY IS THE FOUNDATION OF API PROTECTION

### Discover APIs

- Truly agentless
- Automatic
- Continuous
- Real time
- Discover ALL APIs (including "shadow" APIs)

### Automatically Catalog APIs

- Deep payload inspection
- Capture every spec
- No manual effort
- Maintain catalog
- Create blueprint (records) of API parameters and specs
- Always up-to-date

### Deep API Insights

- Complete dashboard
- API Risks Analysis – identify sensitive data
- Behavioral Insights
- Identify how APIs are connected
- Third party APIs
- Apps with third-party APIs
- Identify unauthorized access



CloudVector Enterprise Edition enables security practitioners to know the unknown, so they can protect what matters most: their data.



## KEY FEATURES AND BENEFITS OF CLOUDVECTOR ENTERPRISE EDITION THAT ENABLE ITS COMPREHENSIVE VISIBILITY INCLUDE:



**All-Encompassing API Discovery:** CloudVector Enterprise Edition automatically and continuously discovers all APIs, even undocumented or unapproved APIs (Shadow APIs). Organizations that use CloudVector to create an API inventory can be confident that it accurately represents their entire enterprise application environment.



**Automatically Catalog APIs:** CloudVector Enterprise Edition delivers deep inspection into API payloads to capture every parameter and specification. By eliminating the manual creation and maintenance of API catalogs, CloudVector Enterprise Edition enables organizations to efficiently create blueprints (records) of API parameters and specifications that remain up-to-date and error-free. Furthermore, these blueprints can be easily exported into other API management solutions.



**Deep API Insights:** CloudVector Enterprise Edition provides a comprehensive dashboard of fine-grained API risk analytics, API behavioral analytics, and API traffic metrics. These insights can be exported into a summary report or integrated into other API management solutions. CloudVector Enterprise enables organizations to make informed decisions about how data flows across its enterprise and what data is at risk, so it can prioritize its data protection policies (available within CloudVector Enterprise Edition).



**API Risk Analysis:** Determine which APIs have access to sensitive data. Identify vulnerable APIs, based on the [OWASP API Security Top Ten](#), such as broken authentication and authorization, and excessive data exposure. Observe API access token risk, including how many APIs a single token is able to access, how many APIs have restless access tokens, and how many APIs lack access tokens entirely.



**API Behavioral Insights:** Determine which APIs bring data into the enterprise, take data out of the enterprise or interact with other APIs (i.e. GET/POST/TRANSACTION). Identify how different APIs are connected to each other.



**API Traffic Metrics:** Determine what percentage of enterprise traffic is via APIs. Identify which APIs are accessed by external users, how many APIs are developed by third-parties, and how many applications use third-party APIs. Obtain visibility into unauthorized access.

CloudVector Enterprise Edition has many benefits beyond discovering what you do not know, such as real-time observability in testing environments and real-time data monitoring in production environments. When it comes to security, CloudVector Enterprise Edition also provides real-time anomaly detection and granular policy enforcement.

Deep API visibility is the foundation of API data security because knowing is half the battle. CloudVector Enterprise Edition enables organizations to automatically and continuously discover its entire API inventory, collect its API parameters, and analyze risk metrics, so that they can efficiently create and maintain API catalogs and prioritize API data protection. **CloudVector Enterprise Edition enables security practitioners to know the unknown, so they can protect what matters most: their data.**