DATASHEET

CloudVector Enterprise Edition

Comprehensive API Security – Complete Visibility and Granular Control

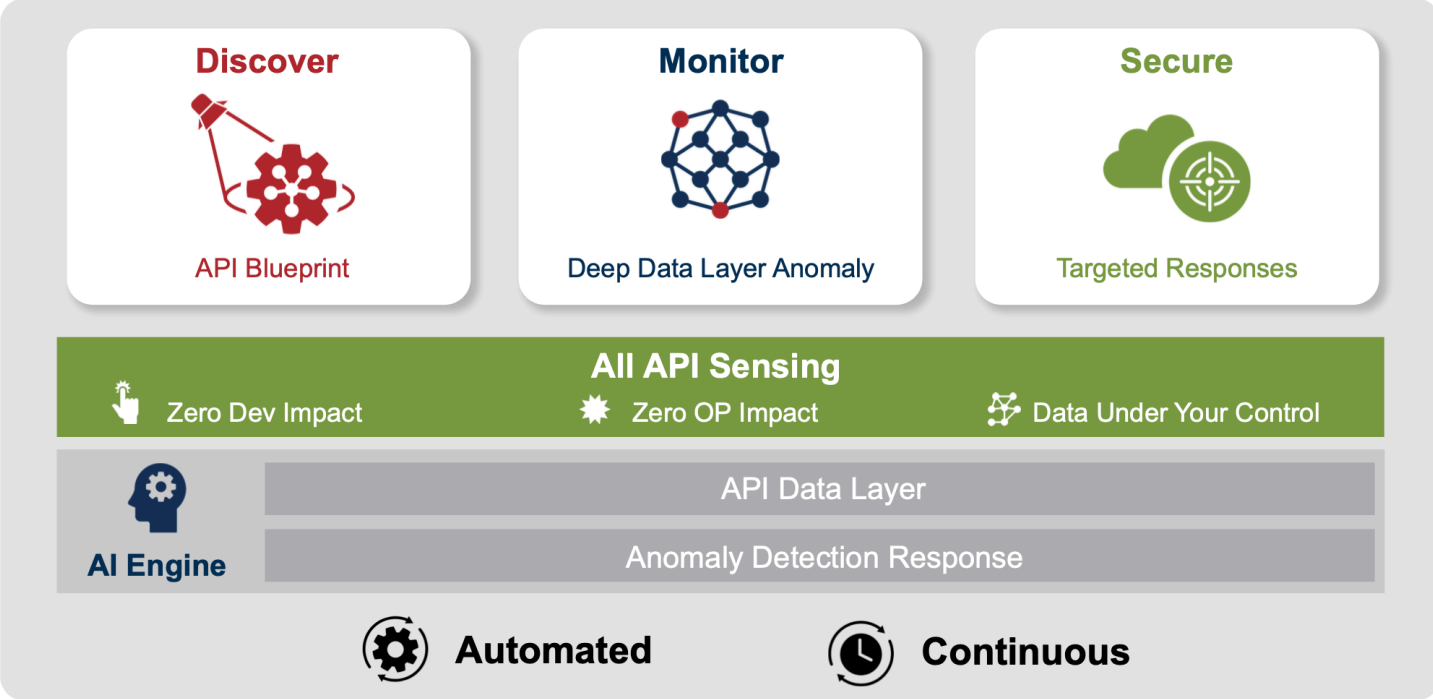
OVERVIEW

- Digital transformation, cloud-based applications, and agile development are driving the proliferation of APIs faster than DevOps and security teams can manage them.
- Web Application Firewalls (WAFs) were not designed for APIs and API management gateways were not designed for security. The result is a massive security blind spot responsible for a new wave of API-based data breaches—from Capital One to USPS.
- CloudVector provides pioneering protection against API risks with its AI-enhanced approach to automatically and continuously discover, monitor and secure all APIs with zero impact to application environments—a solution that mitigates API-based data breaches without causing friction for DevOps.

HOW IT WORKS

CloudVector is a software solution that leverages a unique micro-sensor deployment with zero impact to developers or performance. These smart sensors provide deeper inspection into API parameters than any other solution. Machine learning models behavior for anomaly detection and intelligent automation streamlines policy management to eliminate operational inefficiencies.

- **Discover – Deep API Inspection:** Automatically and continuously catalog high-fidelity blueprints for all APIs—even Shadow APIs.
- **Monitor – AI Behavior Modeling:** Establish a baseline behavior model and compare usage patterns to detect anomalies.
- **Secure – Granular Policy Management:** Automatically apply API controls to block a single session, instead of the entire application.



FEATURES

Continuous API Catalogs
Automatically generate high-fidelity API blueprints for export in OpenAPI (Swagger).

Deep API Inspection
Gain deep insight into API parameters to assess risk.

Discover Shadow APIs
Identify undocumented API specs and out-of-spec behavior.

AI-Enhanced Anomaly Detection
Machine Learning models the behavior of APIs, users and services to monitors for anomalies.

Granular Policy Management
Apply API controls to block a single session – invalidate the access token instead of taking down the entire application.

Intelligent Automation
AI-enabled protection policies prevent API abuse and API-related data breaches.

THE MAP IS NOT THE TERRITORY – CHART THE UNKNOWN

Whether validating an existing API spec or generating an API blueprint from scratch, CloudVector continuously and automatically discovers every single API and provides deep inspection into its parameters. CloudVector even catalogs previously undocumented APIs and unknown Shadow APIs.

SMARTER EVERYDAY – AI AND INTELLIGENT AUTOMATION

The reality is that API management and security can be time-consuming and error-prone processes, which strain resources and introduce risk. CloudVector applies machine learning to create baseline behavior models and intelligent automation of policy management to streamline operations.

A MICRO SOLUTION WITH MACRO BENEFITS

The gap between WAFs and API management gateways may seem as deep and wide as the Mariana Trench, but CloudVector is illuminating this security blind spot with its unique micro-sensors, which are deployed with zero impact to developers or performance and provide the deepest API inspection of any solution.

CloudVector Use Cases

KEEP A WATCHFUL EYE ON APIs

Automatically generate and continuously update a catalog of API blueprints, specifications, and parameters. Validate dev, test and production environments. Identify APIs that are no longer in use.

360° API PROTECTION

Protect “north-south” (public) and “east-west” (internal) API traffic. Mitigate third-party risk. Detect Shadow APIs. Secure exposed applications. Prevent lateral attacks and abuse of trust. Identify access to sensitive data. Block access at a session level.

GOVERNANCE & COMPLIANCE

Trust but verify security operations. Ensure data is encrypted by detecting when secure transport (TLS/SSL) is not in use. Easily collect evidence for audits to demonstrate compliance.