SOLUTION BRIEF | CLOUDVECTOR ENTERPRISE EDITION

Model and Monitor Third-Party API Behavior

Mitigate the Risk of Integrating Third-Party Applications into Enterprise Environments

CLOUDVECTOR

Organizations are on guard after an outbreak of attacks compromised enterprise systems through third-party APIs. Innovative application integration introduces risk as organizations consume and expose a variety of third-party APIs. Most service providers provide no indication of the expected behavior for their APIs. Most organizations lack the tools to monitor third-party APIs. Most security professionals would agree that letting software execute arbitrary code is dangerous, but this is exactly the risk of third-party APIs. If a vulnerable third-party API exists on your system, it may be compromised to spread malicious code or to attack your organization.

CLOUDVECTOR PROVIDES SUPERIOR VISIBILITY INTO THIRD-PARTY API BEHAVIOR

Security organizations are largely blind to the risk of third-party APIs, even if they have tools to monitor internal APIs. Code scanning tools and application development lifecycle management solutions don't work with third-party APIs because of their proprietary nature. It is nearly impossible to test the API surface exposed by third-party applications, especially when Shadow API parameters are unknown even to the service provider themselves. Furthermore, most emerging solutions seem to ignore legacy systems and traditional application architectures.

Conventional Web Application Firewalls (WAF) and/or API Gateways can only detect certain anomalous access patterns or protect against already known attacks. Even an advanced Web Application and API Protection (WAAP) solution is dependent on known API specifications for API data layer validation. In the case of third-party application APIs, these sort of gateway solutions are ineffective because they lack access to the up-to-date API specifications required to operate and are unable to detect hidden or modified parameters.

CloudVector leverages Deep API Intelligence™, machine learning and a unique micro-sensor architecture to deliver the deepest insights, the broadest systems support, and the lightest touch on DevOps. Deep API Intelligence™ reveals the payload of all API calls, even Shadow APIs and third-party APIs. Artificial intelligence and machine learning automatically and continuously discover and catalog API analytics, which it monitors for behavioral anomalies and malicious attacks. Best of all, CloudVector's unique micro-sensor architecture makes it flexible enough to deploy into the most complex and hybrid environments without any changes to third-party code or impact on performance.

FEATURES AND BENEFITS OF CLOUDVECTOR ENTERPRISE EDITION

	Catalog and Categorize APIs	Behavioral Analytics	Real-Time Protection
Features	Automatically and continuously discover all APIs, even Shadow APIs and third-party APIs	Leverages AI and ML to generate analytics Know call features, forensics and identity attributes	Detect suspicious and malicious behavior Enforce granular policy controls
Benefits	Complete visibility into API data flows Know key data attributes	Model API behavior Monitor behavioral anomalies	Detect early signals of attack Terminate suspicious sessions or block applications

KEY FEATURES AND BENEFITS OF CLOUDVECTOR ENTERPRISE EDITION THAT MITIGATE THE RISK OF THIRD-PARTY APIS INCLUDE:

Catalog and Categorize Third-Party APIs: Automatically and continuously inventory the specifications and parameters of all APIs, including third-party APIs and their hidden parameters (Shadow APIs). CloudVector can discover all APIs, even in complex or hybrid environments. Conversely, CloudVector can discover third-party APIs in traditional infrastructure, even if they do not generate logs.

Generate Third-Party API Behavioral Analytics: CloudVector leverages artificial intelligence and machine learning (AI/ML) to generate behavioral analytics for third-party APIs, including its call features, forensics and identity attributes. These insights are available in a summary view, a downloadable report, or for export into other API management solutions.

Call Features: Includes typical request size, frequency, query string, the number of parameters, and their type—even from failed call attempts.

Forensics: Includes IP address, geographic origin, device and browser features, user name, and connections and communication to other APIs.

Identity, Access and Authorization: Identify API calls that have compromised account credentials or bypassed authentication for unauthorized access.

Real-Time Data Protection: CloudVector also leverages its AI/ML engine to continuously monitor anomalies, such as third-party APIs using an unknown parameter or abnormal user access patterns, which may indicate an attack. Granular policy controls can terminate a single suspicious session or block an entire application until it is remediated.

Modern enterprises that have integrated third-party applications cannot go back, but they can mitigate the risk. It is imperative that organizations obtain the ability to gain visibility into third-party APIs since their service providers do not readily provide this information. CloudVector provides this visibility, for internal and third-party APIs, for on-premise, cloud and hybrid environments, so that organizations can understand their risk and respond to attacks.