CEQUENCE

Datasheet

Cequence API Spartan

Bot Management and Fraud Prevention

Bots, both good and bad, generate almost half of all web traffic today. Malicious bots used to primarily target websites and applications, but today they often bypass apps and target APIs directly. The ubiquity of APIs combined with their accessibility, ease of use, and flexibility have made them a top target. Even properly-coded APIs can be subject to business logic abuse as part of a large-scale account takeover (ATO) or shopping bot campaign. Mass fake account creation and content scraping campaigns are regularly executed against applications and their APIs. Organizations need a solution that detects and prevents automated attacks against their applications and APIs, is easy to deploy, and is immediately effective.

API Spartan Overview

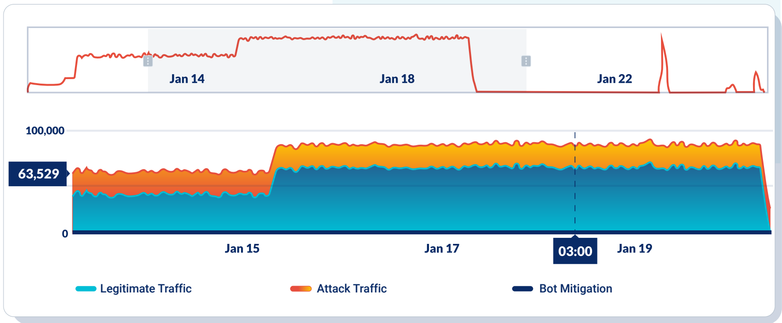
API Spartan is a bot management and fraud prevention solution that protects organizations from the full range of automated attacks to prevent data loss, theft, and fraud. Powered by CQAI, an ML-based analytics engine that determines in real time if application transactions are malicious or legitimate, API Spartan natively mitigates attacks and eliminates harmful business impacts such as downtime, brand damage, skewed sales analytics, and increased infrastructure costs.

API Spartan is part of the Cequence **Unified API Protection** platform or available as separate **Bot Management** and **Fraud Prevention** modules.

API Spartan Features

Continuous Behavior-Based API Threat Detection

API Spartan's ML-based analytics engine analyzes behavioral intent across web, mobile, and API traffic, identifying legitimate and malicious bots based on their behavior, not just their IP addresses. Using this analysis, API Spartan develops behavioral fingerprints that continuously track sophisticated attacks, even as adversaries retool to avoid detection. This highly-effective approach requires no client-side or application integration, ensuring the broadest possible application and API protection.



API Spartan at a Glance

✓ **No application modification**
No server- or client-side agents, JavaScript, or SDK integration required

✓ **Native mitigation**
Attack identification and blocking without relying on third-party infrastructure such as WAFs

✓ **Rapid time to value**
Deploys quickly and is immediately effective

✓ **Flexible deployment model**
Supports on-premises, SaaS, or hybrid

✓ **API fraud prevention**
Customizable, granular policies for organization-specific use cases

Applications and APIs are facing a broad range of brute force and sophisticated attacks, and attackers employ a variety of tools and techniques that are often difficult to detect, not to mention prevent. API Spartan detects and mitigates a variety of attack types, including:

- **Account Takeover (ATO)**
- **BOLA vulnerabilities**
- **Flash sales, hype sales, and sneaker drops**
- **Sensitive data exposure**
- **Gift card / loyalty program abuse**
- **Fake account creation**

Mitigate Attacks Natively and in Real Time

Once discovered, attacks can be mitigated natively with API Spartan, eliminating the need to rely on a WAF or other third-party solution that may not be capable of supporting the attack volume. API Spartan scales elastically and native mitigation ensures latency-free, end-to-end control over attack detection and mitigation. Mitigation options include blocking, rate limiting, geo-fencing, logging, and deception, a technique that misleads the attacker into believing that their attacks have been successful.

Consistent Coverage for All Applications

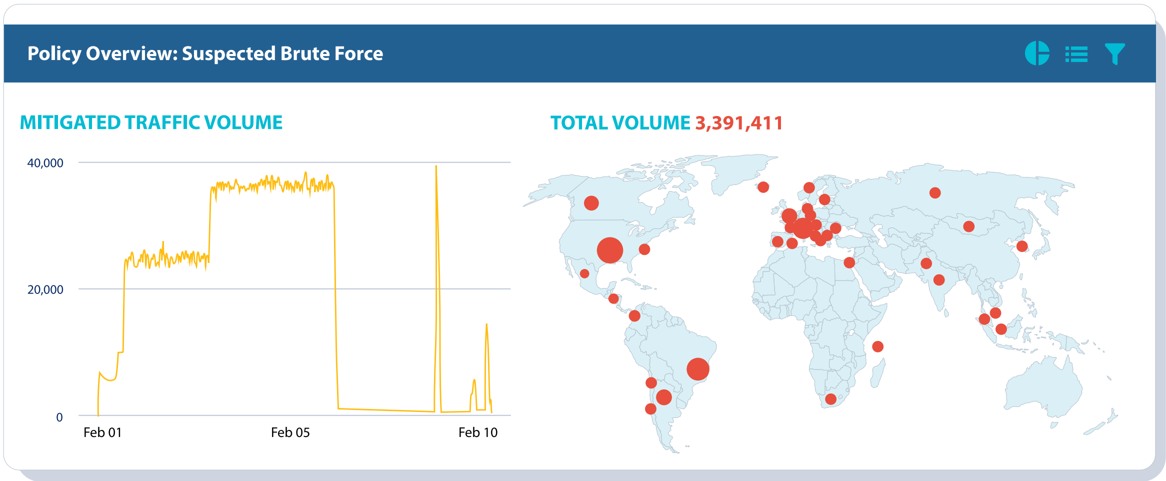
API Spartan protects all application traffic, extending protection beyond applications and infrastructure that support application-specific toolkits, agents, or SDKs to include web applications, mobile devices, and even cloud- and microservices-based architectures. This approach also eliminates the development and testing required by app instrumentation, saving time and effort.

Rapid Time to Value

API Spartan is easily deployed and immediately effective, onboarding new APIs in as little as 15 minutes. There's no application instrumentation to include in the CI/CD pipeline, eliminating a major hurdle faced by competing solutions. It features flexible SaaS, on-premises, or hybrid deployment options to meet business needs.

Fraud Prevention Tailored to Your Business

API Spartan offers a fraud prevention module that supports customizable, granular policies for fraud prevention use cases specific to your business and vertical. As traffic flows to APIs, API Spartan identifies and blocks activity matching those fraud policies in real time and provides detailed information for analysis of each fraud campaign. Out-of-the-box policies can be modified by the customer with no coding necessary, and new policies can be created to meet changing needs.



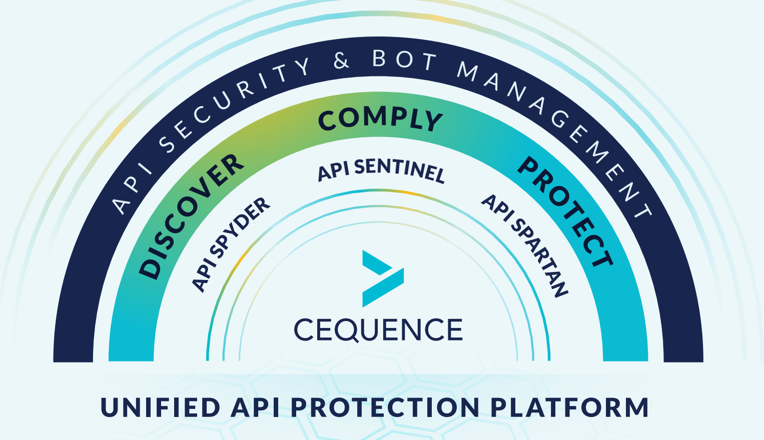
Policy Overview: Suspected Brute Force

MITIGATED TRAFFIC VOLUME

TOTAL VOLUME 3,391,411

API Spartan is Part of the Cequence Unified API Protection Platform

The Cequence Unified API Protection platform unites discovery, compliance, and protection across all applications and APIs to defend against attacks, targeted abuse, and fraud. Discover all internal and external APIs, manage your complete API security posture, repel bot attacks, and prevent fraud – all with a single, integrated platform. Cequence solutions scale to handle the most demanding Fortune and Global 500 organizations, securing more than 8 billion daily API calls and protecting more than 3 billion user accounts. The Cequence Unified API Protection platform also includes **API Spyder** for attack surface discovery and **API Sentinel** for API security posture management.



CEQUENCE

© 2024 Cequence Security, Inc. All rights reserved.