CEQUENCE

Datasheet

Bot Management and Fraud Prevention

Cequence Spartan

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 for threat actors. 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 efforts 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.

Spartan Overview

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

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

Spartan Features

No Application Modification or Customer Friction

Spartan's network-based approach precludes the need for agents or any application modification such as JavaScript or mobile SDK integration. This approach eliminates customer friction induced by bot-prevention methods such as CAPTCHAs and extends coverage to all applications and APIs, and not just those that can be instrumented. Spartan's network-based protection also eliminates the development and testing effort required by app instrumentation, saving time and expense.

Spartan at a Glance

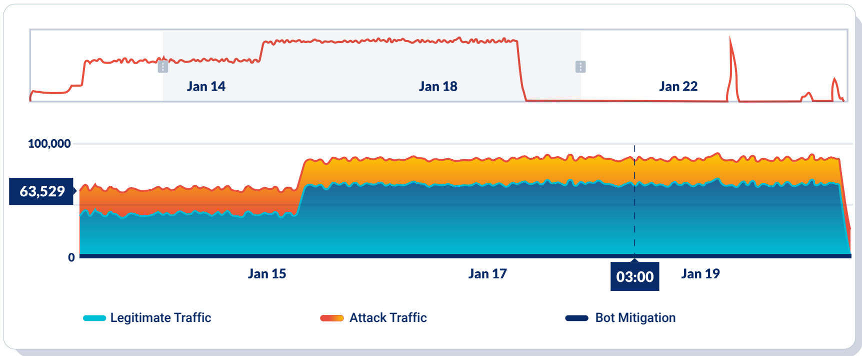
- ✓ **No CAPTCHA Needed —** network-based approach requires no agents, JavaScript, or SDK integration
- ✓ **Native Mitigation —** attack identification and blocking without relying on third-party infrastructure such as WAFs
- ✓ **Rapid Time to Value —** deploys quickly and is immediately effective
- ✓ **Flexible Deployment Model —** supports on-premises, SaaS, and hybrid
- ✓ **API Fraud Prevention —** customizable, granular policies for organization-specific use cases

Organizations may not even know they have a bot problem; bots are simply a way to automate attacks at scale. 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**

Continuous Behavior-Based Threat Detection

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

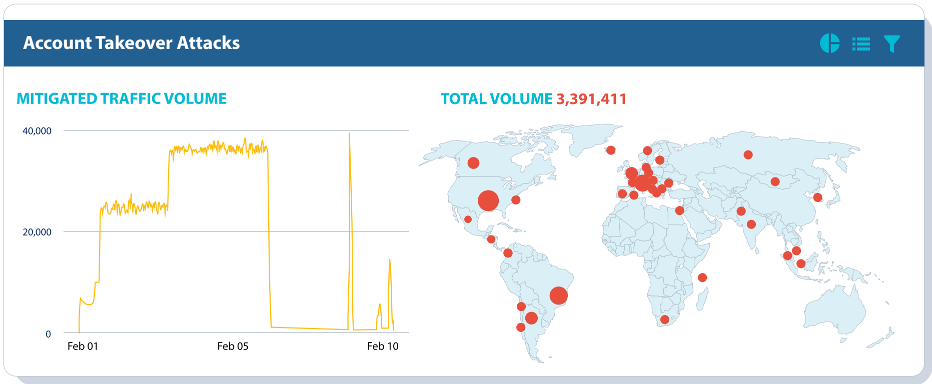


Rapid Time to Value

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, and hybrid deployment options to meet business needs.

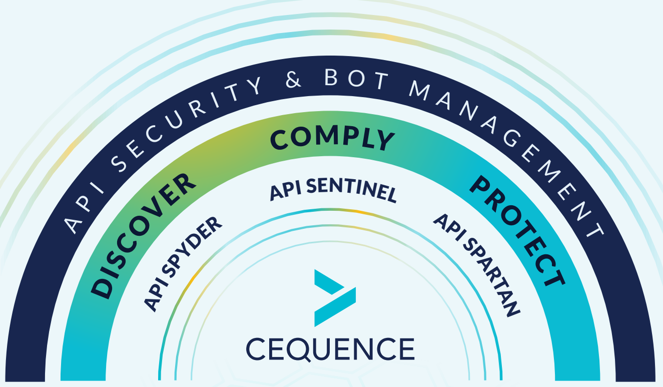
Fraud Prevention Tailored to Your Business

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, Spartan identifies and blocks activity matching those fraud policies in real time and provides detailed information for analysis of each fraud campaign. New policies can be created and out-of-the-box policies can be modified by the customer with no coding required.



Spartan is Part of the Cequence Unified API Protection Platform

The Cequence **Unified API Protection platform** unites discovery, compliance, and protection across all internal, external, and third-party APIs to defend against attacks, targeted abuse, and fraud. Onboard APIs in minutes, without requiring any instrumentation, SDK, or JavaScript deployments. Cequence solutions scale to the most demanding government, 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.



UNIFIED API PROTECTION PLATFORM

CEQUENCE

5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai

© 2024 Cequence Security, Inc. All rights reserved.