CEQUENCE

Datasheet

Cequence Web Application and API Protection (WAAP)

Integrated Bot Management, API Security, WAF, and DDoS Protection

Applications and their associated APIs continue to proliferate and the difficulty of protecting them all against sophisticated attacks is increasing. Organizations are embracing modern architectures and existing solutions simply haven't kept up. With the advent of artificial intelligence (AI), enterprise security requires a comprehensive approach that protects both "normal" and AI-enhanced attacks, whether it's unwanted content scraping, sensitive data exfiltration, business logic abuse, or high-volume attacks designed to disrupt.

WAAP at a Glance

- **Advanced Bot Management** detects and blocks malicious bots
- **Comprehensive API Security** offers posture management and testing
- **Powerful WAF** delivers web application-specific protection
- **Scalable DDoS Protection** intercepts volumetric attacks

Cequence WAAP Overview

Customers have frequently asked us to add Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) capabilities to our existing API Security and Bot Management offerings for a true best-of-breed WAAP solution. Vendor consolidation, cost savings, and overall performance are among the most common reasons. As such, we've added a powerful WAF and highly-scalable DDoS protection to deliver an enterprise-class cloud WAAP capable of scaling to the largest enterprises. Cequence WAAP protects all your web and API applications against sophisticated threats and bot attacks, conventional and AI-enhanced alike, all in a single cloud tenant. This integrated SaaS solution delivers several benefits:

Operational Efficiency

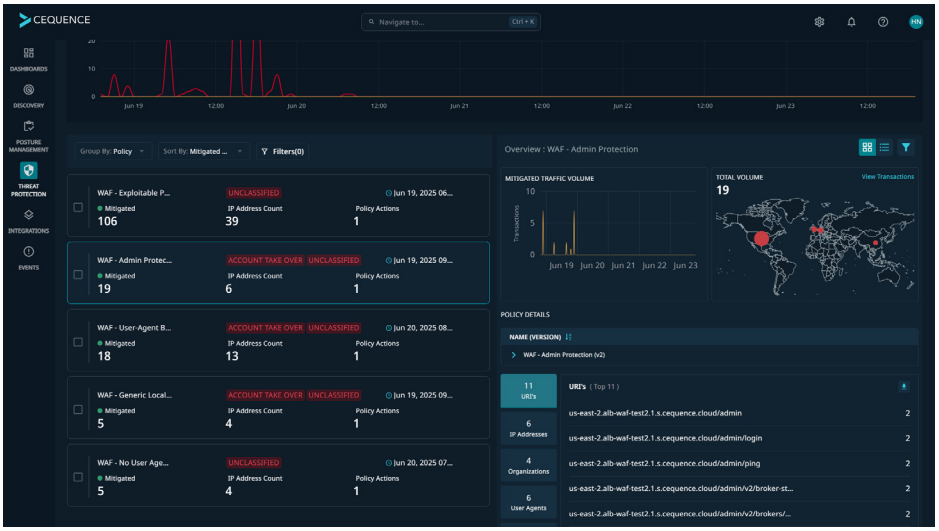
Single application protection portal for WAF, bot management, and API security minimizes admin complexity and overhead

Reduced Latency

Single cloud deployment eliminates multiple cloud hops

Reduced Risk

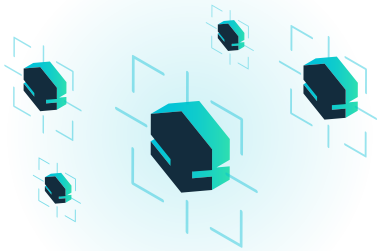
Integrated components within a single cloud tenant eliminate coverage gaps caused by inconsistent traffic routing



Triggered WAF rules are viewable in the Cequence dashboard.

Cequence WAAP Capabilities

Bot Management



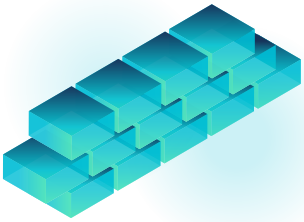
Cequence Bot Management protects an organization's web, mobile, and API applications from both highly sophisticated and volumetric bot attacks. Its network-based approach requires no application modification so time to value is measured in hours rather than weeks. Cequence's behavioral fingerprinting provides industry-leading bot detection (both good and bad) and mitigates attacks in real time out of the box for applications and APIs, preventing data loss, theft, and fraud that cause downtime, brand damage, skewed sales analytics, and increased infrastructure costs.

API Security

Cequence API Security discovers, monitors, and tests your APIs, assessing a broad range of risks that can lead to compliance and governance issues, data loss, and business disruption. Internal, external, and third-party APIs are discovered, and API specifications can be automatically created as needed. Cequence also automatically detects and masks sensitive data, preventing unintended exposure. API security testing finds issues in development as well as runtime, enabling organizations to shift left as they shield right.

Web Application Firewall

The WAF is a powerful and highly scalable solution with a comprehensive set of rules and policies, providing protection against the OWASP Web Application Top 10, malicious input patterns, and SQL injection. Threats detected by the WAF are handled by Cequence Bot Management which has several mitigation options including blocking, rate limiting, header injection, and deceptive responses. Detected threats are tagged by the WAF and integration with Cequence Bot Management enables real-time protection, improves WAF performance by offloading mitigation, and provides a single console for managing WAF activity and bot management.

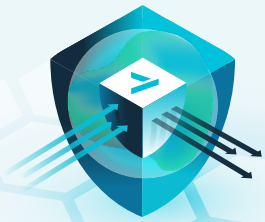


DDoS Protection

Highly-scalable DDoS protection ensures applications and APIs are shielded against even the largest DDoS attacks that would otherwise overwhelm infrastructure and disrupt business operations. It protects resources from volumetric attacks such as reflection attacks (layer 3), network protocol attacks such as SYN floods and UDP floods (layer 4), as well as application and API layer attacks (layer 7). The solution is highly resilient and offers 99.99% availability against common infrastructure attacks.

Deployment

Cequence WAAP can be deployed in a Cequence Cloud tenant or the customer's AWS tenant. Cequence also offers a Managed WAAP with all components fully managed and monitored by Cequence. Leveraging AWS' worldwide presence ensures close geolocation of the cloud tenants, regardless of the customer's location.



WAAP and AI

AI is changing the game when it comes to enterprise security, but it's leveraging existing communication channels. Cequence WAAP already protects your applications and APIs, so you can be sure that even as AI evolves, you remain secure. Cequence also offers an AI Gateway, the easiest and fastest way to connect agents and enterprise and SaaS applications.

CEQUENCE

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