Cequence ASP

An Extensible, Open Platform for Stronger Security, Improved Productivity

The Cequence Application Security Platform (ASP) represents a revolutionary approach to application security that protects all of your externally-facing applications, whether web, mobile, or API, from bots and targeted threats. Unlike other solutions, Cequence ASP requires no modification to your web or mobile applications and even discovers applications and APIs that you may not have known existed.

The ASP software platform is integrated with three key components: the CQAI Analytics Engine, CQ Manager, and CQ Connect. The heart of the platform is CQAI, which uses its unique position in the network to deliver advanced AI and machine learning-based threat detection and analysis that continually adapts to changing attacks. Sensors collect a copy of relevant network traffic, then CQAI correlates across client, network, application, and behavioral contexts. This provides a complete understanding of every user interaction to distinguish humans from bots, and benign actions from malicious actions. CQ Manager provides security teams with attack insights and enables options for real-time blocking, rate limiting, and active attack deception to prevent damage to your organization and assets. Finally, CQ Connect leverages open APIs to share relevant data with your SIEM or anti-fraud teams for ongoing correlation and analysis.

Full Coverage For Your Application Attack Surface

Organizations don't get to choose which applications are attacked. Today, every app and interface that needs protection requires incremental effort from security teams to add JavaScript, modify SDKs, and continually tune rules and signatures. This requires time, manpower, and invariably leads to gaps in coverage.

Cequence ASP turns this model on its head. Using a distributed, software-only architecture, Cequence is deployed once and automatically discovers and protects all of an organization's applications, including web, mobile, or APIs as well as any hidden apps or interfaces. The solution requires no changes at all to applications, doesn't impact performance, and supports local or cloud-based applications without the need for appliances. This secure-by-default approach means that applications remain secured even as developers roll out new APIs or spin up new interfaces. As the application environment changes, security coverage scales horizontally with no additional effort from security staff.

Cequence ASP Advantages

- AI/ML-based protection from bots, ATO, scraping, and business logic attacks
- Deployable on-premises, in the cloud, across multiple locations, and without appliances
- Automatic discovery of all applications across all locations
- One solution to defend web, mobile, and API everywhere
- No need for application modification using JavaScript or mobile SDKs
- Intent-based detection to distinguish threats from benign automation
- Per-app blocking, prevention, and deception
- An open system with the ability to create connectors to other security tools

Protection From Orchestrated Application Attacks

Cequence ASP arms security teams to automatically detect and repel the incredible volume and diversity of attacks that applications face on a daily basis. With new patent-pending AI and machine-learning, the CQAI engine can identify malicious actions down to the level of intent, without the need for signatures and manual tuning. As threats evolve, the CQAI engine automatically adapts without the need for managing signatures.

The CQAI engine is modular and extensible. As Cequence develops new security modules, the platform can easily add detection and protection for additional classes of threats.

Malicious Automation

More than 30% of all Internet traffic is malicious bot activity and another 20% are legitimate bots. When paired with the CQ botDefense security module, the CQAI engine automatically separates the human from automated traffic and the malicious from benign. This allows Cequence to stop automated attacks such as account takeovers (ATO), content scraping, fake account creation, business logic abuse, and other types of fraudulent behavior. However, not all automation is bad, and the advanced AI of the CQAI can track behavior down to the level of intent to distinguish between malicious bots and benign forms of automation such as approved aggregators.

Mitigation and Deception

When attacks are detected, Cequence ASP works with Cequence service modules like CQ botDefense to provide a variety of blocking, deception, and rate limiting responses that can be triggered based on policy.

Deception techniques offer a particularly powerful counter to automated threats. The benefit of deception is two-fold. In addition to preventing attacks from consuming valuable application resources, deception can also lure attackers into believing that they have succeeded. For example, Cequence could allow an attacker to believe that a credential testing attack succeeded, while security staff continues to monitor and learn the attackers behavior and intent.

The mitigation engine can provide a variety of nuanced operational responses. Suspicious new accounts can be routed to the accounts team for monitoring or investigation. Fraudsters scraping pricing information can be fed fake or inaccurate information, while real customers continue to see real prices.

Attack Types

- App DDoS
- Account takeover
- Content scraping
- API/Business logic abuse
- Fake account creation
- Reputation compromise
- Automated shopping / Denial of inventory

Additionally, CQ Connect allows Cequence to trigger actions in other security devices such as a WAF or SIEM. For example, the Cequence F5 Connector can dynamically create F5 iRules to block threats. These options allow security teams to apply the appropriate type and level of response to the threat to ensure that their apps and data stay safe and valid users are not impacted.

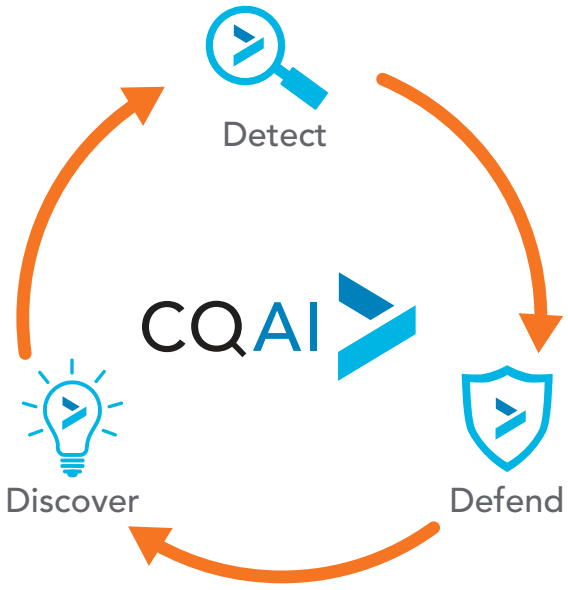
The Cequence ASP Architecture and Components

Cequence ASP introduces a unique approach, architecture, and intelligence that enable the platform to defend applications in ways other WAF and bot defense solutions can't.

Simple Network Deployment

First, Cequence deploys in the network where it can passively analyze all traffic between clients and the application server. This position allows Cequence to see all traffic destined for the application regardless of what web page, mobile interface, or API the client is using. All paths lead to the application, and Cequence inserts sensors at the point where it can see all of this traffic, without making any changes to the application.

Cequence ASP logically separates the roles of detection and enforcement, allowing detection to be passive and enforcement to be active. This separation of duties ensures that the solution can perform in-depth, long-term analysis of all application traffic without any impact or added latency to the application. Also, when malicious or suspicious traffic is detected, Cequence can block, rate-limit, or actively deceive live attack traffic.



CQAI Engine - Multidimensional Adaptive AI

CQAI's distributed sensors and centralized analytics give it access to a rich, comprehensive set of data and context for analysis. Instead of relying only on client-side telemetry, CQAI analyzes every interaction from a client, network, and application perspective. For example, while client-facing analysis may reveal header-based anomalies, an application-side analysis can reveal more specific attack behavior, such as an attacker repeatedly putting a product in a cart but not purchasing as part of a denial of inventory attack.

With this multidimensional perspective, Cequence then applies an ensemble of artificial intelligence, machine learning models, behavioral analysis, and statistical analysis to identify automation and threats. The approach blends header analysis, protocol analysis, user and application behavior, and ongoing statistical analysis across hundreds of traits. By combining multiple detection strategies and perspectives, Cequence can correlate and confirm threats without having to rely on a single algorithm or heuristic. For example, a visitor using a VPN might have user agent anomalies that would trigger a false positive in traditional heuristics, while CQAI would recognize that the actions are still valid based on the user's behavior, application, and network responses.

CQAI even distinguishes behaviors down to the level of intent. For example, the platform can allow a valid content aggregator while blocking a malicious ATO campaign even though the high-level behaviors can appear similar. When a threat is identified, the CQAI engine builds a fingerprint of the threat based on attack tools, infrastructure, and behavior so that staff can recognize and easily track the threat over time. In the end, CQAI provides a multidimensional analysis that enables it to find threats other solutions would miss, while also reducing false positives.

Multidimensional AI

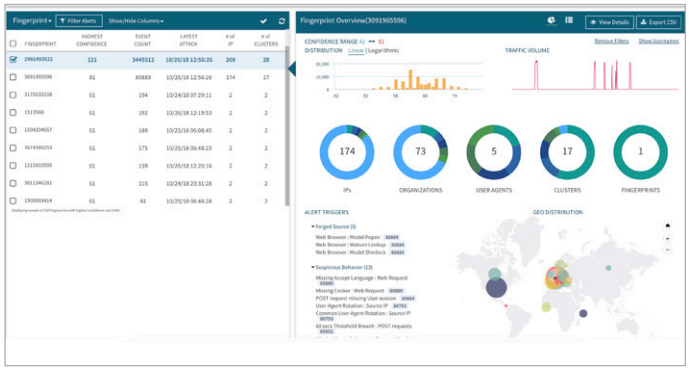
- **AI-based detection with no signatures to manage**
- **No additional network latency from detection**
- **Unified context combining application, client, and network**
- **Intent-based detection to reveal true malicious behavior**

CQ Manager - Actionable Insights for Fast Response

The CQ Manager provides the interface to the platform, allowing staff to investigate incidents and manage policies. First, the CQ Manager gives staff insight into the application environment and all discovered applications. Cequence's automated discovery of applications often reveals apps that were not previously being monitored, and allows staff to identify any newly deployed applications easily. This is especially helpful in decentralized IT environments and large enterprises.

Next, CQ Manager provides detailed insight into application and attack traffic. Staff can easily track valid traffic and attack traffic over time, and hone in on particular events and times of interest. Statistics and behaviors can be analyzed at a variety of levels from individual IP addresses to ASN, ISP, or geographical areas. When staff needs to investigate a particular event, they can dive into any incident to see the detailed metadata and logic behind a detection for easy confirmation and investigation.

CQ Manager also allows security staff to respond to threats in a manner most appropriate for the business. This is achieved through policies, which dictate what action(s) to take when malicious traffic is detected. Policies can be set to have different responses for different applications. For example, account takeover attempts can trigger deception responses, whereas fake account creation can stream the detected list of fake accounts to the risk/fraud team. Likewise, you can contain the impact of financial aggregators by using traffic shaping.



CQ Connect - An Open, Extensible Platform

While many security products are so-called "black boxes," Cequence ASP is an open system by design that shares details and empowers your analysts and data scientists. In addition to traditional logs and alerts, analysts can access the detailed signals and metadata behind CQAI detections to correlate with their other systems and feeds. The solution natively integrates with Jupyter notebooks so that data scientists can work with Cequence data in their own environment. Cequence even allows teams to write their own custom logic and algorithms to run in CQAI. This open design allows Cequence to be a bi-directional hub of intelligence that empowers the rest of the organization instead of just being another source of logs. The inverse is also true - you can feed the CQAI additional security intelligence or leaked credentials for monitoring. This lets enterprise leverage their investments in security intelligence and anti-fraud systems by connecting them to the Cequence ASP platform.

Flexible Deployment

Cequence easily deploys into most any environment, whether applications are deployed in a local datacenter, in the cloud, or in a hybrid environment. Cequence software is deployed as a Docker container making it straightforward to deploy in a variety of environments. Traffic is delivered to Cequence for analysis typically via a TAP port in a physical network environment or via NGINX Plug-In in a cloud deployment.

Product Specifications

Server Hardware

- Cequence recommends the following hardware:
- CPUs: 64-bit Intel CPU
- Hard Disk Type: SSD
- Network Interface: Dual Intel 1Gb/10Gb NICs

Server Software

- The Detector & Mitigator require the following software:
- Red Hat Enterprise Linux 7 (64-bit) or higher / CentOS 7 (64-bit) or higher
- Docker: Enterprise or Community Edition version 17.06.0 or higher, and Docker Compose for the installed Docker version
- Python 2.7.x

You can also learn more about the Cequence Application Security Platform by visiting our website's resources section: cequence.ai/resources.

CEQUENCE™ SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-408-978-3258 › info@cequence.ai › www.cequence.ai