Cequence Application Security Platform (ASP)

AI-Powered Platform for Stronger Application Security

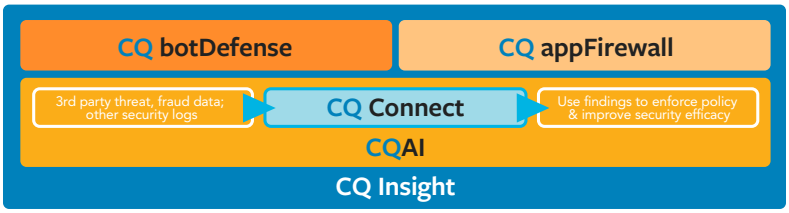
Introduction

Today's hyper-connected businesses rely on a broad set of web. mobile, and API-based applications to connect customers, partners, and suppliers across the Internet. Retirement planning, interacting with likeminded hobby enthusiasts, loyalty program participation while purchasing our favorite goods and services are just a few examples. These applications incorporate a wide range of application endpoints, such as a registration, login, or forgot user name and password pages.

Recognizing the insatiable user demand for a richer, online user experience, organizations are adopting more rapid and iterative application development methodologies, allowing them to extend their competitive edge. Oftentimes, development moves more quickly than security. Each new public facing web, mobile, and API-based application or feature release, expands your attack surface, allowing bad actors to use automation, attack frameworks and stolen user credentials from the dark web to target these public facing applications. Traditional approaches to protecting them are largely ineffective and are hard to manage, requiring regular updates as applications are deployed and updated. What's needed is an innovative, platform-oriented approach that provides you with complete visibility and actionable intelligence to protect your modern application infrastructure.

Cequence Application Security Platform

The Cequence Application Security Platform (ASP) takes an intelligence-based approach to protecting your web, mobile and API-based application infrastructure from automated attacks, malicious bots, and exploits. Cequence ASP is a distributed, container-based architecture that is scalable and flexible, allowing you to integrate security into your application infrastructure. Cequence ASP is comprised of the following elements:



Cequence Application Security Platform

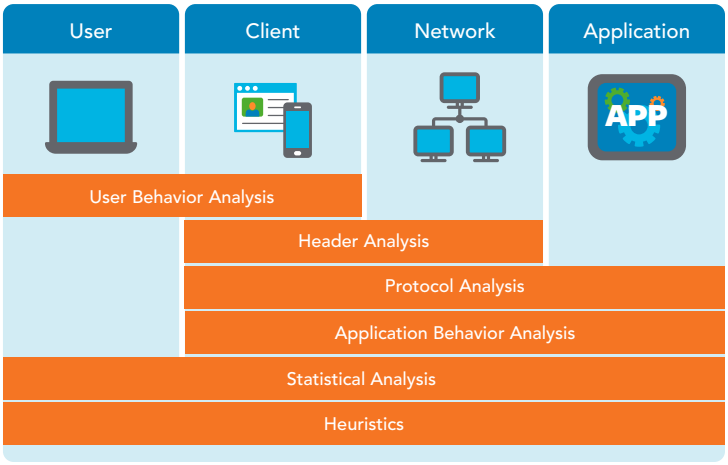
- CQAI is the patented intelligence engine for the platform, using machine learning and analytics to automatically discover your web, mobile and API-based applications while uncovering threats and vulnerabilities that may lead to application infrastructure compromise and/or data loss. CQAI uses multiple techniques to analyze your transactions to provide you with a more complete view of application and threat behavior than other technologies that rely on client context alone. Applications and threats identified by CQAI can then be used to drive policy creation and enforcement within two security modules:
  - CQ botDefense uses the intelligence generated by CQAI to determine the actual intent of the application transactions, allowing you to protect all your public facing web, mobile and API-based applications from a broad range of business logic abuse attacks typically orchestrated using bots or human farms.
  - CQ appFirewall takes full advantage of CQAI to intelligently extend traditional WAF functionality to address one of the most significant WAF deficiencies: the inability to detect and prevent unknown, or zero-day attacks.

› **CQ Connect** enables you to easily integrate Cequence ASP into your existing security infrastructure, allowing you to ingest 3rd party data to augment CQAI findings, or send CQAI findings to your existing security tools to improve the efficacy of your existing security tools and productivity of your security team.

› **CQ Insight** is the centralized management tool that provides unmatched visibility into your web, mobile and API-based applications wherever they are deployed, allowing you to understand the intent of the traffic and take appropriate mitigation actions.

CQAI: Multidimensional AI-Based Application Visibility and Threat Detection

CQAI analyzes every interaction from a user, client, network, and application perspective. This multi-dimensional analysis provides you with a complete view of behavior – far more than what is possible with technologies that rely on client context alone. For example, while client-side analysis can reveal unusual header anomalies, application-side analysis can see the actual attack behavior of a denial of inventory attack where a user repeatedly puts items in his basket without purchasing.



CQAI then uses an ensemble of machine learning models, behavioral analysis, and statistical analysis of hundreds of traits to build a syntactic profile of the application used to identify threats and to facilitate policy creation. This includes, but is not limited to, heuristic analysis of headers, protocols, other network traffic, and both user and application behavior. CQAI also performs a statistical analysis of all of these traits to identify patterns and anomalies. By tracking the unique multi-step behaviors of real attacks against your applications, CQAI distinguishes malicious bots from benign forms of automation such as approved content aggregators.

The Cequence threat research team continuously analyzes dark web activity, attack tools and techniques, and compromised networks to ensure that CQAI is regularly updated with the intelligence needed to provide superior detection and defense. For example, CQAI works in concert with two Cequence security modules, CQ botDefense to prevent malicious bot attacks and CQ appFirewall to prevent known and zero-day vulnerability exploits.

CQ botDefense: Detect and Respond to Business Logic Attacks

When CQAI discovers an attack, a fingerprint is created that includes attack tools and infrastructure used along with exhibited behavior that helps to ensure continued protection via CQ botDefense. The fingerprint allows you to track the attackers in near real-time, even if they use a single IP address or continually move to new IP addresses. By blending multiple perspectives and types of analyses, CQAI provides an accurate, low-impact approach that detects threats others miss while reducing false positives.

Responses are automated by policy, and range from blocking to rate limiting, to highly customized active deception. Deception offers a particularly powerful counter to automated attacks and can make an attacker believe a credential stuffing attack was successful. This disrupts the attack, feeding bad data back to the attacker, allowing security teams to observe the attackers next steps and long-term intent, all while preventing the attacker from consuming resources of the actual application.

CQ appFirewall: Developer Friendly Application Security

CQ appFirewall complements CQ botDefense, using the intelligence generated by CQAI to address common compliance requirements such as protecting against the OWASP Top 10 and supporting PCI DSS Section 6.6. CQ appFirewall then goes beyond commodity WAF functionality to accomplish two key goals. First and most importantly,

because CQ appFirewall understands how the application works, it addresses a glaring hole in application security – the ability to prevent zero-day vulnerability exploits that may lead to data loss or infrastructure compromise. The second goal that application profiling accomplishes is it allows application security to be an integral step in the development workflow by minimizing, and sometimes eliminating the administrative effort associated with signature creation.

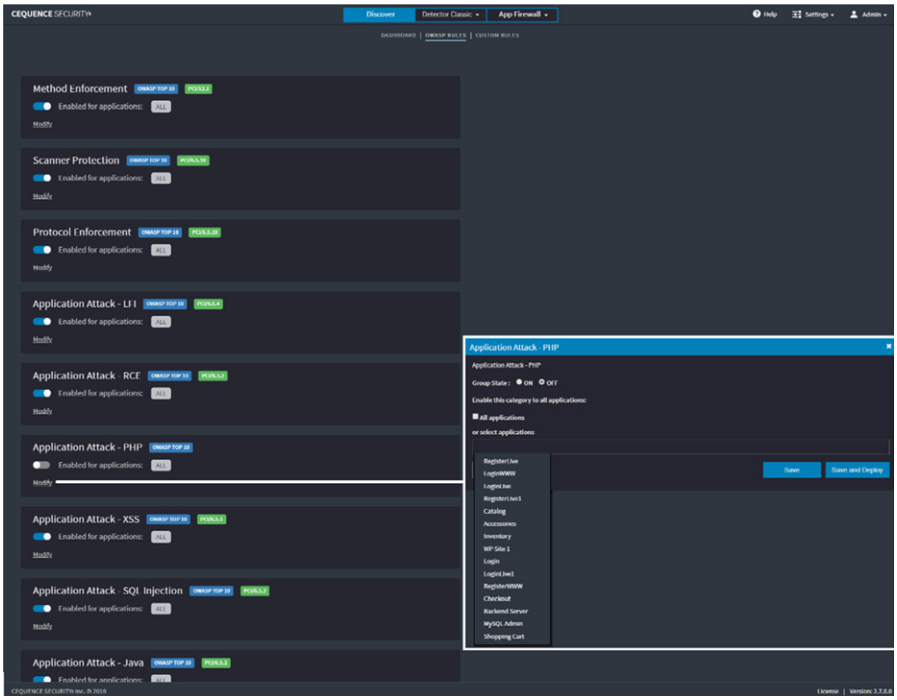


Image 1: CQ appFirewall includes predefined rule categories for key OWASP and PCI requirements.

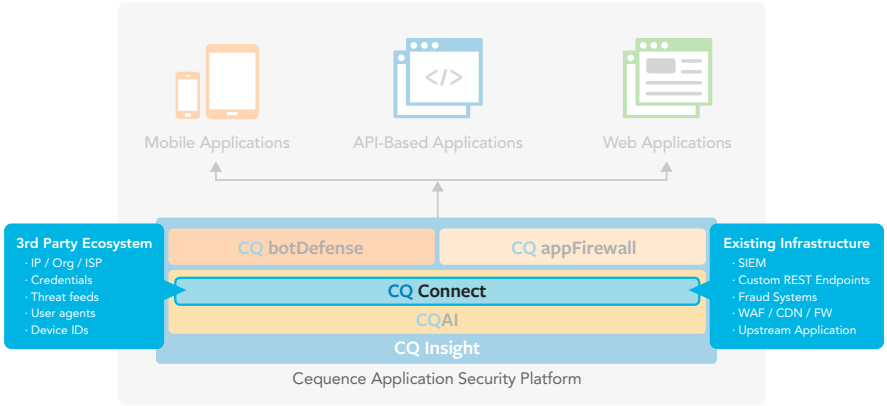
As enterprises execute their cloud-centric application initiatives, human errors that can result in data exposure from misconfigurations or inadvertently using a common application with a known vulnerability continue to be challenges for the security team. CQ appFirewall automatically discovers mis-configured applications that may be exposing data to the web, allowing you to apply pre-defined policies to protect those applications. Predefined signatures for commonly used (and targeted) applications such as WordPress, Drupal, Apache and Microsoft IIS helps minimize or eliminate the potential damage that an exposed vulnerability may cause. Custom applications are treated in a similar manner – they are analyzed to create a fingerprint which can be used to determine if it is under attack and then take action to mitigate it.

In the event that an attack is detected by CQ appFirewall, administrators can choose from a range of mitigation options that include, alert, block, geo-fencing, and deception. Using deception as a mitigation technique is unique in that if fools the bad actor into believing the attack has been successful.

Application profiling, predefined applications and templates combined with a distributed, container-based architecture allows application security to be easily embedded into the application development workflow. New applications and updates can be deployed as needed and Cequence ASP will begin protecting them, without requiring security change control requests, application instrumentation or SDK modification.

CQ Connect: Enrich Findings and Improve Security Outcomes

To improve the efficacy of your existing security infrastructure, CQ Connect uses an open API that allows you to send CQAI findings to your firewall or WAF for enforcement, or to your SIEM for additional analysis. CQ Connect also allows you to ingest 3rd party data from threat and fraud subscriptions or from your SIEM as a means of enhancing the CQAI findings.



CQ Insight: Turning Actionable Intelligence into Policy

CQ Insight is the centralized management tool that provides visibility into your applications, their transactions, and any threats that may be hiding in plain sight. Armed with the knowledge of what the intent of your web, mobile and API-based application traffic is, you can build policies to protect your digital assets. Policy examples can include:

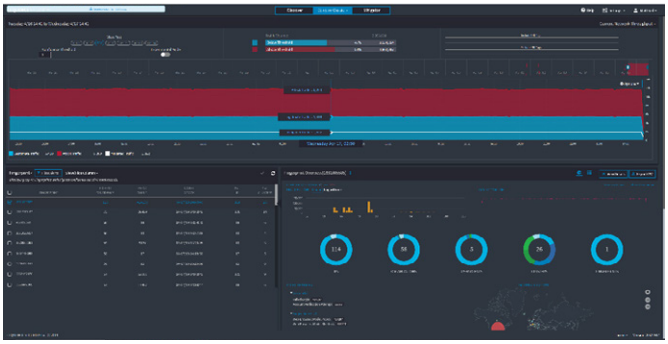


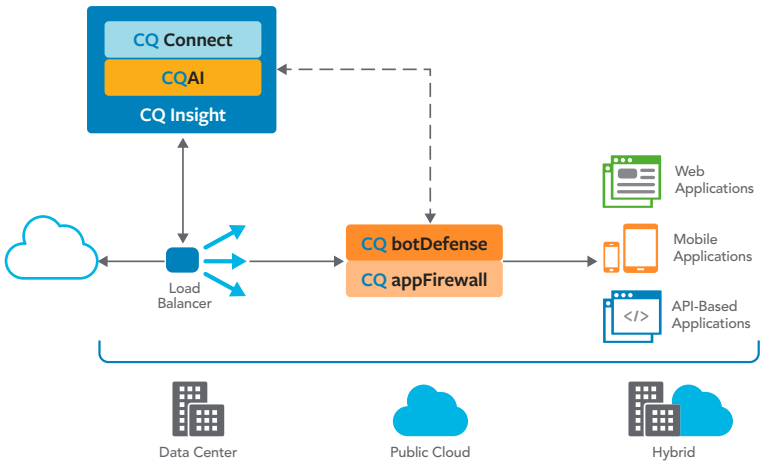
Image 2: Visualize your application traffic and take action on attacks with CQ Insight.

- Preventing account takeovers and subsequent reputation bombs for social media applications.
- Stopping denial of inventory and seat spinning for retail or airline reservation systems.
- Protecting financial services applications from account takeovers and subsequent theft.

In addition to a visual summary of your application traffic and the attacks that may be targeting them, CQ Insight gives you the ability to create custom rules, enable and disable system rules, and configure all aspects of Cequence ASP. Rules created and deployed by CQ Insight leverage the continual analysis performed by CQAI to ensure new attacks are detected automatically, thereby minimizing or eliminating the need for to monitor Cequence ASP 24x7.

Cloud-Native Architecture for Deployment Flexibility

Cequence ASP is a distributed, container-based architecture that can be deployed in public cloud, data center and hybrid environments. CQ botDefense and CQ appFirewall are deployed as a single component in the line of traffic, sending traffic to CQ AI and taking action as dictated by policy. Small and lightweight to ensure low latency and minimal impact, CQ botDefense and CQ appFirewall are designed to fail-open in the event of a failure. CQAI, CQ Connect and CQ Insight are deployed in a central location, performing analysis, providing visibility, dictating policy and enriching the existing infrastructure through CQ Connect import/export capabilities. This distributed approach to deployment allows organizations to quickly and easily support their ever-evolving public facing application infrastructures.



Cequence Application Security Platform

About Cequence Security

Cequence Security is a venture-backed cybersecurity software company founded in 2015 and based in Sunnyvale, CA. Its mission is to transform application security by consolidating multiple innovative security functions within an open, AI-powered software platform that protects customers web, mobile, and API-based applications – and supports today's cloud-native, container-based application architectures. The company is led by industry veterans that previously held leadership positions at Palo Alto Networks and Symantec. Customers include F500 organizations across multiple vertical markets, and the solution has earned multiple industry accolades. Learn more at www.cequence.ai.

CEQUENCE™ SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai