Introduction
Data breach announcements resulting from the use of a web application component that has an unpatched vulnerability have become a regular occurrence. Historically, organizations have addressed these risks using a Web Application Firewalls (WAF), focusing on the OWASP Top 10 and helping to address PCI regulatory compliance. Unfortunately, attack advancements and the move towards more rapid and iterative application development methodologies have rendered WAFs ineffective at protecting your public facing application infrastructure. WAFs are hard to manage and their traditional change control approach to signature and policy updates can introduce delays into the application development lifecycle, which often impacts user experience.

CQ appFirewall takes a new approach, one that uses intelligence and automation to extend far beyond traditional OWASP Top 10 and PCI DSS Section 6.6 focused WAF functionality. CQ appFirewall complements CQ botDefense as the second, newest security module available within the Cequence Application Security Platform (ASP).

Cequence Application Security Platform
The Cequence Application Security Platform (ASP) protects your web, mobile and API-based application infrastructure from automated attacks, bots, and exploits.

The intelligence of the platform resides with CQAI, a patented machine learning, analytics engine that automatically discovers your web, mobile and API-based applications while uncovering threats and vulnerabilities that may lead to application infrastructure compromise and/or data loss. This provides 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 within two security modules:

- **CQ appFirewall** leverages CQAI to intelligently extend traditional WAF functionality simplifying administrative effort with predefined application profiles and policy templates while improving security with the ability to prevent unknown, or zero-day attacks.
- **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 business logic abuse attacks typically orchestrated using bots or human farms.

Additional Cequence ASP elements include CQ Connect and CQ Insight, which allow you to more easily integrate the platform with your existing security infrastructure and to perform centralized management, respectfully.
CQ appFirewall: Applying Intelligence to Application Security

CQ appFirewall takes an intelligence-based approach to extend beyond static, signature-based based techniques used by commodity WAFs to accomplish several key objectives common across most organizations:

› Simplifies management, enabling your team to do more with less. CQ appFirewall fully leverages intelligence generated by CQAI to virtually eliminate the need to manually create and update applications and threat signatures.

› Improves security efficacy with customizable application infrastructure defense. Threat response options that go beyond traditional alert and block, CQ appFirewall allows you to improve security efficacy with creative mitigation techniques such as geo-fencing and deception.

› Integrates with your existing security infrastructure. As an integral component of Cequence ASP, CQ appFirewall takes advantage of CQ Connect to share information and thus improve the efficacy of your entire security infrastructure. The distributed, container-based architecture enables you to deploy CQ appFirewall in the cloud, data center or hybrid locations.

› Enables application security consolidation. Managed centrally, the integrated elements of the Cequence ASP, CQ appFirewall and CQ botDefense allow you to consolidate multiple application security functions – bot protection and application firewall – into a single pane of glass.

CQ appFirewall addresses the vulnerability protection and compliance requirements (e.g., OWASP Top 10 and PCI DSS Section 6.6) that most organizations already have in house – but have struggled to make effective even after years of use. The key difference is that CQ appFirewall is a module integrated within Cequence ASP. This eliminates many of the issues associated with implementing and operating web application firewalls – issues stemming from being in-line, capacity problems, difficulty deploying and maintaining the right rules in place. Furthermore, since Cequence ASP can consistently protect web, mobile apps, and API-based applications, CQ appFirewall can protect an organization’s entire modern application landscape.

Application Intelligence Reduces Administrative Effort

CQ appFirewall uses the patented CQAI multidimensional, machine learning analysis to fully understand your commercial and custom web, mobile and API-based applications, building a syntactic fingerprint that you can then use in multiple ways, accomplishing more with less effort.

First and foremost, the fingerprint is based on the continual analysis of your applications, CQ appFirewall 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 application fingerprint is used in a policy template and as the application is updated, it can be deployed as needed and automatically protected, without requiring security change control requests, application instrumentation or SDK modification.

To further reduce the administrative effort associated with application security, CQ appFirewall includes predefined rules distributed across predefined categories as well as profiles for commonly used (and

Image 1: CQ appFirewall includes predefined rule categories for key OWASP and PCI requirements.
exploited) commercial applications. Out of the box application profiles include WordPress, Magento, Drupal, Joomla, Apache, and Microsoft IIS with more added over time. Using the predefined profiles and policy templates will help ensure that your organization is protected from all-too-common zero-day vulnerabilities found in some of these applications.

A regular source for many of today’s security incidents is human error which result in data exposure from misconfigurations or inadvertently using a common application with a known vulnerability. CQ appFirewall automatically discovers misconfigured applications that may be exposing data to the web, allowing you to apply pre-defined policies to effectively lock them down thereby preventing data theft. For example, if Elasticsearch has been deployed and inadvertently configured to be publicly accessible via the web, CQ appFirewall will automatically discover that error and initiate a policy-based response.

**Improve Security Efficacy with Customized Application Defense**

Attacks detected by CQ appFirewall can be mitigated with response options that extend beyond traditional signature-based blocking. Mitigation options include traditional responses such as alert, block, rate limiting, and geo-fencing based on countries listed by the US Treasury Department Office of Foreign Assets Control.

Using deception as a mitigation technique goes beyond traditional response mechanisms. Deception as a mitigation technique allows you to convince the attacker that their malicious efforts have been successful. A deception-based response disturbs the economic factors surrounding the attack, thereby impacting the ability for an attacker to achieve their monetary objectives. For example, if credential validation and resale on the Dark Web is the attack objective, deception will tell the bad actor that the credentials are valid and can be sold for a premium. In reality, the credentials would be fake, and essentially worthless.

The third way in which you can respond to an attack is to use a bot fingerprint mitigation technique such as whitelisting or header injection. These response options are used when the application attack is volumetric, incorporating automation to take advantage of the respective vulnerability.

**Tighter Integration for a Stronger Security Infrastructure**

Too often, security solutions are closed systems, unable to easily export information or import 3rd party data to improve overall security efficacy. CQ Connect, an integral element of Cequence ASP is an open API that allows you to send information on the attack to your existing 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.

Organizations are adopting cloud-native initiatives to leverage the benefits of agility, scalability and near immediate access to compute, networking, storage and a rich application infrastructure. Available globally, these resources can quickly expand to meet regional needs, or scale out to meet performance or capacity demands. Further fueling this momentum are iterative and agile application development methodologies that leverage containers, microservices and Kubernetes as an orchestration tool that allow your new applications and updates to be deployed more quickly.
To fully support your hyperconnected application environment, Cequence ASP uses a distributed, container-based architecture that allows you to deploy security wherever your applications are located – in the public cloud, the data center, or hybrid. CQ appFirewall is deployed in conjunction with your load balancer so that it is close to the application, sending a copy of the traffic to CQAI for analysis and action as dictated by policy. A small and lightweight module to ensure low latency and minimal impact, CQ appFirewall is 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, executing 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.

Consolidating Application Security with CQ appFirewall and CQ botDefense

Industry estimates are that malicious bots represent 35% of all web traffic. In some Cequence customer environments, 90% or more of web traffic has been associated with malicious bots. CQ appFirewall and CQ botDefense deliver on the promise of “better together,” allowing our customers to improve their application security posture and consolidate multiple security functions. CQ botDefense blocks malicious bot traffic, immediately reducing your threat footprint and the load on your infrastructure associated with malicious bot traffic. CQ appFirewall will then enforce policy to prevent data loss and infrastructure compromise brought on by vulnerabilities in your commercial or custom applications.

Security that’s Baked into your Application Infrastructure

Cloud-native initiatives typically entail moving towards container and micro-services application development methodology that is more agile and iterative. In these scenarios, security must keep pace, moving beyond traditional change-control oriented approach that often introduces delay into the application development workflow. CQ appFirewall allows your team to use profiling, predefined applications and policy templates to bake security into your application infrastructure. CQAI continually analyzes your applications to ensure that new applications and updates can be deployed as needed and Cequence security modules within the platform will begin protecting them, without requiring security change control requests, application instrumentation or SDK modification.
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:

- Quickly add policies to address OWASP Top 10 requirements.
- Protecting commonly used commercial applications like Apache from known and zero-day vulnerabilities.
- Using deception to respond to and mitigate a credential validation attack.

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 add and modify custom rules, enable and disable system rules, and configure Cequence ASP.

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.