CEQUENCE

Top 10 Criteria
to Consider When Going WAAP Shopping

The Web Application and API Protection (WAAP) product space was originally identified by Gartner Research in a piece published in October of 2017. While eight years may not seem like a long time, given the rate at which the cybersecurity threat landscape evolves, it's an eternity. At the time, Gartner considered WAAP to be a natural evolution of the traditional Web Application Firewall (WAF) products. The core WAAP capabilities Gartner identified include:

- **Web Application Firewall** acts as a protective layer between web applications and the internet, filtering traffic based on predefined security rules to block malicious activity like SQL injection and cross-site scripting (XSS)

- **Distributed Denial of Service (DDoS) protection** continuously monitors network traffic to detect and block malicious requests before they overwhelm a target

- **Bot Mitigation** defends applications and APIs by detecting and mitigating malicious automated traffic (bad bots) while allowing legitimate bots (like search crawlers) through, preventing attacks, business logic abuse, and fraud

- **API Security** which involves securing API infrastructure based on discovery, schema enforcement, and behavioral analysis

Because of the rate and sophistication at which automated attacks on applications and APIs have developed, the decision criteria that thoughtful cybersecurity professionals use to choose a WAAP solution have also evolved. While WAAP is an established product category, there are innovative solutions and vendors to be found within it…if you know what to look for.

Below is the list of the top ten considerations that should *currently* be used to evaluate a new WAAP solution.

1.
Demonstrable Effectiveness

Ultimately, effective cybersecurity is about how well mitigation measures do in stopping adversaries from compromising sensitive information and business operations. In the case of bot "management" it's not just about distinguishing human from synthetic users but about distinguishing malicious synthetic users from benign ones like search engine crawlers. A track record of proven detection accuracy is key.

> Historically enterprises have relied on legacy IP source detection mechanisms or client-side CAPTCHA's which have proven vulnerable to AI based attacks. Cequence Bot Management utilizes machine learning and advanced behavioral analytics to consistently detect attacks and fraud and natively mitigate in real time. Cequence Bot Management is deployed with 150+ customizable rules that identify attacks and provide immediate mitigation.

2.
Threat Coverage

In the current threat landscape being able to identify the OWASP Top 10 is the bare minimum and not even close to a complete solution. Lists like the OWASP Top 10, MITRE's CVE list, and even CISA's Top 15 are lagging indicators of the state of the threat landscape in the same way that the Oscars and Emmys honor LAST year's best movies and television shows. These are necessary but insufficient databases from which to operate an effective threat detection system.

Cequence WAAP starts with those lists and adds AI-driven intent analysis to detect attacks, business logic abuse, and fraud. Besides providing customers with superior visibility on emerging threats, the Cequence threat team also provides active threat response services.

3.
Ease of Deployment

If a solution requires each application to be modified, rollout will be painfully slow and incomplete. Worse, as business systems are upgraded or swapped out it means that the instrumentation and testing process must be replicated with each change to the IT infrastructure.

Cequence WAAP is network based, requiring no agents or application modification. It integrates seamlessly into existing infrastructure on-premises, in the cloud, or in hybrid configurations. And once deployed, Cequence WAAP scales elastically, processing traffic far faster than competing solutions.

4.
Ease of Management

Gartner originally defined WAAP as consisting of four different components. Conceptually this is the right approach, but disjointed management can make it complicated and expensive to manage. Be wary of siloed management consoles that slow down management and dilute effectiveness.

Cequence WAAP provides a single control plane for admins to view which attacks were blocked by which component (WAF or Bot Management) and a single place from which to manage the system.

5.
Customization Options

No two enterprises run exactly alike. Businesses require customizability to properly support geographic and regulatory differences, industry standards, and legacy business practices.

Cequence establishes a customizable baseline of business logic and sensitive data based on how the business operates and how data is transacted. Based on that, it can, for example, detect industry-specific sensitive data to automatically mask, preventing it from being unintentionally exposed.

6.
Support & Maintenance

Many WAAP solutions are unintegrated point products, often assembled via acquisition. They have different code bases, different management interfaces, and generally are difficult to support and manage.

Bot management and API security is the core of Cequence Security's mission, not a sideline. Deploying Cequence WAAP is just the start of our relationship with global enterprises. We pride ourselves on providing "white glove" customer support services which customers frequently cite as standing out in comparison to their experience with other vendors.

7.
Demonstrated Scalability

Many WAAP vendors claim their products are highly scalable, but do they have customers with large deployments that demonstrate that scalability?

Cequence's network-based approach enables its products to scale to the largest and most demanding organizations. Some customers process over 1 billion transactions a day, all protected by Cequence.

8.
Visibility

Many WAAP solutions operate as "black boxes", reporting what threats are mitigated but not why. This lack of visibility increases the likelihood that legitimate customers and traffic are inadvertently blocked.

Cequence WAAP provides clear visibility into what triggered a mitigation and enables cybersecurity teams to easily and quickly update rules as needed. Cequence AI/ML can suggest appropriate detection rules and mitigation policies for human review, or if desired, put them in place automatically.

9.

Best of Breed Components

Gravitate toward solutions with a shared architectural foundation, avoid WAAP solutions that have grown inorganically with one strong component surrounded by “second tier” components.

> Cequence WAAP is an integrated solution made up of industry-leading components that work together to optimize security outcomes. And does so without requiring the management of separate user consoles or disparate vendors.

10.

Protection Against Future Threats

The advent of artificial intelligence means the threat landscape is now more dynamic than ever. Just because a WAAP can address today’s threats does not mean it will recognize future AI-driven threats as they emerge.

> Cequence products use AI and ML to detect and track threats and even to autonomously create policies and mitigate attacks without human intervention. Cequence researchers use AI disciplines to investigate a broad spectrum of potential threat vectors so that protection for these new classes of attacks can be built into the Cequence product suite before they strike.

The Cequence Advantage

Choosing a WAAP solution is not just about blocking attacks – it’s about enabling digital trust, agility, and growth. The Cequence Security WAAP solution is unique in that it offers threat detection, mitigation, and visibility of active threats against application and API attacks. Cequence WAAP also offers a degree of customization unavailable from any other solution. Regardless of whether it is deployed on-premises or as a turnkey service, Cequence WAAP users receive white-glove services to ensure not only a successful deployment but long-term successful security outcomes.