LINK11

WEB APPLICATION API PROTECTION BUYER'S GUIDE

How to Select the Right Web Application Security Solution

www.link11.com

Businesses adapt their digital infrastructures to the changing global environment. As they invest in infrastructure, they also need to consider their web application security.

With business workloads, applications, services, and data increasingly exposed on open internet platforms, investing in a robust web application security solution is more critical than ever. The right solution should not only defend against today's relentless and ever evolving threats but also anticipate and adapt to the challenges of tomorrow. It is now more important than ever to invest in a web application security solution that provides adequate protection against today's advanced and aggressive threats.

This guide explores best practices for evaluating web application security solutions and selecting one that provides a holistic approach to securing your web applications, scales with your business needs, and adapts to emerging threats.

Key criteria to consider when evaluating web application security solutions:

1. Security coverage and depth of the solution
2. Bot protection and traffic insights
3. Effectiveness and sophistication
4. Unified solution for all WAAP pillars
5. Simplifying security with managed services

1. SECURITY COVERAGE AND DEPTH OF THE SOLUTION

A wide variety of web application security solutions are available on the market, generally classified into three categories:

- Native tools offered by cloud service providers (CSPs)
- Single-focus products
- Unified platforms

1. Native tools

The built-in CSP tools are simple to onboard and use. However, they are not well-suited for protecting web applications hosted on different cloud platforms and businesses may also face vendor lock-in risks. While they offer some security measures, they do not provide comprehensive protection, with limited depth and features compared to solutions from specialized security providers.

2. Single-focus products

Standalone security products such as Web Application Firewalls (WAFs), provide deeper functionality than CSP tools, but address only specific aspects of web application security. Organizations must integrate multiple solutions from different vendors to mitigate the wide range of threats, which increases complexity, administrative overhead, and interoperability challenges.

3. Unified Platforms:

While many platforms claim to offer complete security, they are often sold as bundled services with additional costs for essential features such as module upgrades, advanced threat intelligence feeds, extra subdomains, and SSL certificates. Businesses end up paying more than they need to, compared to buying a more cost-effective solution.

For Full Protection in Today's Threat Landscape, a Unified Solution is Essential.

To effectively defend against evolving cyber threats, organizations require a comprehensive, flexible web application security platform that delivers end-to-end protection. This includes a next-generation WAF, multi-layer DDoS protection, bot management, API security, Account Takeover (ATO) prevention, among other critical defenses.

An effective web application security solution should offer:

Full-scope protection – Protection against the full spectrum of modern web threats, ensuring robust security across all attack vectors.

A unified WAAP platform – A fully integrated, all-in-one solution covering all Web Application and API Protection (WAAP) pillars, simplifying security management.

Reduced complexity – A centralized platform for managing all security controls, streamlining operations and minimizing administrative overhead.

Granular policy control – Fine-tuned security policies that allow for precise threat mitigation, reducing false positives and negatives.

2. BOT PROTECTION AND TRAFFIC INSIGHTS

Bots play a role in most web attacks, and threat actors continually develop new ways to evade detection. Organizations need a reliable way to detect and block hostile bots from their sites, applications, and APIs. As a result, filtering malicious bots from incoming traffic is a critical component of modern security.

Traditional bot mitigation techniques include:

- Signature recognition
- Rate limiting
- Blacklisting
- JavaScript injection and cookie handling
- CAPTCHA and reCAPTCHA challenges

While these methods remain effective against older bots, they fail to detect more advanced, AI-driven bots designed to bypass traditional security measures.

These bots use a variety of evasion techniques, including:

- **Spoofing user agent strings** and employing deceptive behaviors to mimic legitimate human users.
- **Executing low and slow attacks** that remain undetected by standard rate-limiting techniques.
- **Using headless browsers** to simulate real user environments, including handling cookies and executing JavaScript.
- **Automatically solving CAPTCHA challenges**, rendering them ineffective.
- **Impersonating mobile applications**, making traditional security methods ineffective for mobile traffic.

Look for a solution that includes technologies for detecting the latest-generation bots. These include:

1. Advanced browser verification – Detects headless environments and automation tools using biometric analysis, client certification mechanisms, and other techniques to verify that incoming requests originate from legitimate sources.

2. Interactive & non-interactive bot challenges – Accurately detects even the most sophisticated bots while maintaining a seamless user experience.

3. Mobile application traffic threat protection – Provides security measures specifically designed for mobile app traffic (e.g. a mobile SDK), where traditional browser-based threat detection methods are not applicable.

4. Advanced rate-limiting mechanisms – Evaluates multiple attributes beyond just IP addresses to detect and mitigate abuse.

5. Behavioral Analysis – Compares current user activity to a baseline of legitimate user behavior.

6. Client certification mechanisms – Verifies that incoming requests originate from legitimate sources.

3. EFFECTIVENESS AND SOPHISTICATION

Many web application security solutions only show blocked requests and often provide limited insight into why those requests were denied.

While this approach can be sufficient in some cases, it can be problematic during security events or even normal traffic conditions, where partial visibility limits your ability to understand and address what's happening.

When comparing web application security solutions, a vital aspect is often overlooked: **traffic visibility**.

When comparing web security solutions, a vital aspect is often overlooked: traffic visibility.

In today's complex threat environment, complete visibility is essential. Organizations need full access to every incoming request —whether blocked or allowed—along with detailed information about its content and context.

This visibility ensures you can understand why decisions were made, identify anomalies, and fine-tune your system to reduce false positives and false negatives. Over time, this increases the precision and effectiveness of your web application security.

Full traffic transparency is vital for maintaining a strong and adaptive security posture.

To provide complete visibility, a web application security solution must include:

- Visibility into content and metadata for each HTTP/S request.
- Clear information about what happened to the request, and why.
- Easy access to current and historical data.
- The ability to build sophisticated queries and gain insights from historical traffic patterns.
- Real-time visibility of both blocked and passed requests.

4. UNIFIED SOLUTION FOR ALL WAAP PILLARS

A WAAP (Web Application and API Protection) solution can be offered either as an integrated platform that combines multiple capabilities, or as individual, standalone solutions.

For comprehensive protection, a robust security posture needs to include the four pillars of WAAP :

1. **WAF (Web Application Firewall):** Protects web applications by filtering and monitoring HTTP/S traffic.
2. **Web DDoS Protection:** Safeguards web applications from Distributed Denial of Service (DDoS) attacks.
3. **Bot Management:** Identifies and mitigates malicious bot traffic while allowing legitimate bots through.
4. **API Protection:** Secures APIs from threats such as unauthorized access, data theft, injection attacks, input fuzzing, vulnerability scans, and ATO (account takeover) attacks.

Standalone solutions may address specific needs, but a unified platform that encompasses all WAAP pillars offers significant advantages. It simplifies management, reduces operational complexity, ensures seamless integration between components, and often results in better overall can improve both performance and cost efficiency.

5. SIMPLIFYING SECURITY WITH MANAGED SERVICES

Implementing a web application security solution isn't a one-time task; it requires continuous management and oversight. Security solutions run the gamut of management options: from none, to paid management & support, to all-inclusive fully managed solutions.

However, there are certain obstacles that hinder the effective configuration and management of these solutions:

Time:
Security management is a time-consuming process. Beyond initial deployment, ongoing maintenance includes updating the solution, adjusting rules, and monitoring for any anomalies.

Complexity:
The threat landscape is constantly evolving. With cybercriminals becoming increasingly well-resourced, it's difficult for organizations to keep up with the pace of new threats. Meanwhile, the modern web provides high financial incentives for cybercrime.

Expertise:
In an era of increasingly sophisticated attacks, managing a security solution requires a high level of expertise, and this standard is continually rising. It is expensive and challenging for many organizations to dedicate sufficient resources to this, and maintain the required in-house expertise.

In-house management of a security solution is neither simple nor inexpensive, and ultimately it might not even be effective. To solve these problems, many organizations are moving to Managed Security Solutions.

Rather than having an in-house team maintaining their platforms, these organizations are letting the security vendor(s) manage them.

This solves all the issues noted above and has many other benefits as well.

- Security vendors offering managed services have dedicated 24/7 support teams that can handle any request, big or small, immediately, and most issues can be solved instantly via a quick phone call or a brief email.
- An all-in-one platform (e.g. next-gen WAF, DDoS protection, Bot management) can simplify security management and save time and money by consolidating multiple services under one provider.

Managed services can also extend beyond traffic filtering, offering additional efficiency gains, such as handling SSL certificates, DNS records, and more. This can save both time and money for organizations by offloading these tasks to the security provider.

CONCLUSION

In the modern threat environment, robust web application security is crucial. A variety of solutions are available, but they are not equal.

Significant differences exist in effectiveness, flexibility, privacy, visibility, pricing, and more. Organizations that perform their due diligence when evaluating solutions can enjoy substantial savings while simultaneously maintaining a stronger and more performant security posture.

Selecting the right WAAP (Web Application and API Protection) solution is key to protecting digital infrastructure against today's sophisticated threats. A unified platform provides comprehensive protection across all WAAP pillars, while simplifying management, reducing operational complexity, and ensuring scalability to meet future needs.

ABOUT LINK11

Link11 is a global cloud security provider offering Network Security, Application & API Protection, and Application Performance solutions to a wide range of industries. From comprehensive Network DDoS protection to an advanced WAAP solution, our platform includes Web Application Firewall (WAF), Web DDoS Protection, Bot Management (including ATO), API Protection, and Secure CDN & DNS.

Link11's DDoS protection solution defends organizations against even the most sophisticated attacks, providing zero-time-to-mitigate for known threats and mitigation in less than 10 seconds for unknown attack vectors.

Get a Demo

LINK11

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | www.link11.com