INDUSFACE™

8 Key Considerations

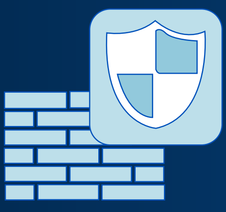
in Choosing the Right Web Application Firewall

Watch Out!

Are you aware that cyberattacks are becoming increasingly complex and sophisticated in the digital age?

A Web Application Firewall (WAF) is the best way to protect your business and customers from today's top threats. A good web application firewall must be armed with the ability to protect your web application from all kinds of known and emerging threat vectors.

Today there are numerous WAFs in the market, each with their own merits and drawbacks. Use these key criteria to evaluate and determine the right WAF to safeguard your business:



1. Detection and Protection Capabilities

The WAF you choose must be equipped to detect and stop all common threats beyond the OWASP Top 10. Its detection and protection capabilities must cover bot protection, business logical flaws, zero-day threats, DDoS attacks, and virtual patching.

2. Scalability and Coverage

The WAF must scale protection with the business and with traffic surges to ensure always-on security and availability of apps. The application firewall must be capable of protecting any type of application – static page, a simple blog, a dynamic website or an e-commerce app and must support API security and security of server-less applications.

3. Customizability

The WAF, while utilizing automation and AI to stop known attacks, should be managed by security experts. This is critical to ensure that the security policies are tuned and customized to secure business logic flaws and unknown vulnerabilities.

4. Deployment

The web firewall must be able to provide effective protection in any deployed environment – public, private, hybrid, or multiple clouds. If you manage multiple sites/ apps, ensure that the solution provides multitenancy to protect all apps/ sites with a single solution.

5. Compliance and Reporting

Choose a WAF solution that enables you to gather data and insights and effortlessly generate reports and documentation necessary for audits and regulatory purposes required to meet compliance standards.

6. Observability and Visibility

The WAF must provide full and continuous visibility into the organization's security posture. For maximum effectiveness and efficiency, it must come equipped with security analytics and a comprehensive, user-friendly dashboard for IT security teams and developers to assess the security status and take corrective action.

7. Managed Services

A managed WAF like AppTrana is recommended to avoid failure. Managed WAFs are equipped with benefits such as expert knowledge and skills, prioritization of cybersecurity, agility, regular updates, global threat intelligence, and dedicated time to ensure tight security.

8. Cost and Support Services

The ideal app firewall vendor must have a transparent pricing strategy with no hidden costs. It must also provide 24*7 support to resolve your security issues.

Secure Your Business Now

Indusface's AppTrana is a fully managed, risk-based application protection solution. It is a comprehensive, and intelligent WAF that detects risks continuously, ensures round-the-clock availability, and total visibility into your security posture.

Contact us now to schedule 14 Days Free Trial.

indusface.com