INDUSFACE ™

Know What You Are Missing with Your
WAF Providers

Not all WAF providers effectively and proactively secure your website/web application. Here is a list of power-packed features that your WAF must have but you may be missing with your WAF providers.

1 The Web App Firewall must be comprehensive to ensure all known vulnerabilities are detected from across the application, server, third-party resources and immediately patched

2 Must be intelligent, equipped with AI, ML, and Global Threat Intelligence Database

3 Security measures, including WAF rules must be customized with surgical accuracy for the unique business needs

4 Must be continuously tuned to keep with the dynamism of the application itself and the emerging threats

5 Backed by certified security experts support to conduct business logic vulnerability assessments, pen-tests, and security audit to strengthen the security posture of the website

6 Must be easy, flexible, and hassle-free to deploy, ensuring zero downtimes for on-boarding

7 Assure zero false positives to ensure that the limited and precious bandwidth of the developers isn't eroded in something that is not a threat

8 Must provide proactive, instantaneous, multi-layered, and tailored protection to your web applications against DDoS attacks of all kinds

9 Must have a comprehensive dashboard that provides security insights and real-time, 24×7 visibility of your risk posture and business impact

AppTrana is a solution that provides all the above power-packed features and is trusted by 1100+ global business clients.

www.indusface.com