Intelligent Web Application Firewall (iWAF)
Point-and-Click Simplicity for Web Application Security

WEB APPLICATIONS ARE UNDER-SECURED BY TODAY’S WAFS
Web application firewalls (WAFs) are intended to protect businesses from web app attacks and proactively prevent threats. Yet, despite the potential security benefits, 90% of organizations find it complex to implement WAF solutions for three key reasons:

• **Complex rules.** Most WAFs today are very complicated, presenting a wall-of-knobs to administrators in order to configure security policies. Tuning rules is even more challenging, not to mention customizing for each application.

• **No visibility or intelligence.** Most WAFs today provide little visibility and lack attack behavior modeling and application learning. Once rule sets are defined, it is difficult to update, monitor and impossible to react in real time to changes or new security threats.

• **Slow to scale.** Traditional WAFs are inelastic and unable to provide the scalability required for increasing volumes of encrypted traffic and variable loads. Hardware appliance-based WAFs need significant overprovisioning.

SOLUTION — AVI IWAF
Avi features an Intelligent Web Application Firewall (iWAF) with a distributed application security fabric to enforce security through closed-loop analytics and application learning mode. iWAF covers OWASP CRS protection, support for compliance regulations such as PCI DSS, HIPAA, and GDPR, positive security model, and signature-based detection. The built-in solution provides security and networking teams with a comprehensive security stack including DDoS, rate limiting, SSL/TLS encryption and ACL that simplifies policy customization and scales automatically on-demand across any environment. See Figure 1.

OPERATIONAL INTELLIGENCE THROUGH MACHINE LEARNING
Avi features an Intelligent Web Application Firewall (iWAF) with a distributed application security fabric to enforce security through closed-loop analytics and application learning mode. iWAF covers OWASP CRS protection, support for compliance regulations such as PCI DSS, HIPAA, and GDPR, positive security model, and signature-based detection. The built-in solution provides security and networking teams with a comprehensive security stack including DDoS, rate limiting, SSL/TLS encryption and ACL that simplifies policy customization and scales automatically on-demand across any environment. See Figure 1.

CHALLENGES
• Increasing complex process for writing security policies and rules
• Lack of visibility into how policies impact traffic flows
• Low performance and massive variability result in scaling and capacity planning challenges

BENEFITS
• Point-and-click simplicity for policies with central security management
• Granular security insights on traffic flows and rule matches to create precise and custom policies
• Elasticity with on-demand autoscaling, optimized security pipeline and per-app protection

FIGURE 1: iWAF Comprehensive Security Stack and Insights
Avi’s iWAF gives administrators end-to-end security insights and analytics on performance, end-user interactions and security events in a single dashboard (Avi App Insights) for actionable insights on security intelligence and enforcement. With Avi PULSE Services, live threat updates including IP reputation, signatures and more are sourced from industry leading threat analysis companies and curated through the Avi PULSE. It protects web applications from common vulnerabilities, such as SQL Injection (SQLi) and Cross-site Scripting (XSS), while providing the ability to customize the rule set for each application. iWAF analyzes the unvalidated traffic through the acceptlist engine, positive security model that validates known good behavior as applications and attack patterns are learned and last the signatures engine processes security rules that match a particular transaction – all these in real-time. The optimized security pipeline maximizes efficiency, sharply reduces false-positives and blocks zero-day attacks. See Figure 2.

**Features at-a-glance**

**Core Security**
- OWASP Top 10 attack protection including HTTP validation, injection, data leakage protection, automated attack blocking and application specific security.
- Guided false-positive mitigation with customizable paranoia levels that control the strictness of the policy based on the logs and analytics.
- Rate-limiting per app to limit L3/L4 and L7 traffic based on parameters such as Client IP, URL and Path.
- Point-and-click policy with central control and ease of use by enabling users to create custom policies quickly and efficiently.
- RBAC support to control write access to WAF profiles and policies; read access to applications, pools, and clouds.

**Threat Detection**
- Acceptlist rules that allow bypassing WAF with known good sources. E.g: Allow DAST scanner IPs from WAF inspection, to exclude internal IP addresses from WAF inspection or to bypass WAF for all POST requests.
- Signatures protection against known threats through a negative security approach by analyzing every part of the incoming and outgoing requests against SQLi, XSS and other threats based on Core Rule Set (CRS).
- Automated threat updates. Sourced from industry leading threat analysis companies Avi Pulse Services continuously updates the iWAF thread database with IP reputation, signatures, and more, protecting web applications from common and new vulnerabilities.

**Application Protection**
- Positive Security Model rules define allowed application behavior and can be created automatically by the learning engine through sampling acceptlist traffic or manually.
- Per-app deployment for precision protection of specific applications with different security policy levels while ensuring application performance.
- On-demand autoscaling to elastically scale the number of WAF instances and application servers to handle unpredictable traffic without impacting performance.
- Application analytics for WAF events based on historical trend information and real-time visibility into ongoing operations, application behavior analysis, and attack patterns.