

VMware® Avi™ Load Balancer Web Application Firewall (WAF)

Modern App Security with Point-and-Click Simplicity

Challenges

- Protect web applications from AI-fueled web attacks with shorter patch window.
- Limited visibility into application performance, traffic flows and security policies.
- Rigid bolt-on legacy appliances that are inelastic, complex and difficult to manage.

Solution — Avi WAF

- Plug-and-Play VMware Cloud Foundation (VCF) integration offers automated deployment and complete life-cycle management.
- Instant Virtual Patching shields web applications from AI attacks at the application edge.
- Integrated multi-layer protection offers DDoS mitigation, rate limiting and bot management.
- AI-assisted behavioral learning protects web applications from false positives.
- Out-of-the-Box compliance streamlines regulatory audits including PCI, HIPAA and GDPR.
- Elastic On-Demand autoscaling automatically scales WAF capacity to handle traffic surges and DDoS attacks.

Need for Modernizing App Defense in the AI-Era

Modern apps face a wave of AI-fueled web attacks and rigid, legacy Web Application Firewalls (WAF) cannot keep up. While the WAF can proactively block these threats, over 90% of organizations struggle with deploying and operationalizing WAF. Those organizations that still depend on legacy web security solutions fail against today's fast, voluminous exploits for three reasons:

- **Complex manual management:** Traditional WAFs present an intimidating "wall of knobs" that requires manual policy configurations. Without AI-driven automation, tuning and customizing rules for individual, evolving applications becomes an impossible chore.
- **Limited visibility:** Legacy WAF solutions lack real-time application visibility and AI-assisted behavioral learning models and fail to stop AI-powered attacks.
- **Slow to scale:** Legacy WAFs are inelastic and require costly overprovisioning for traffic spikes failing to meet modern apps demands for fluid, AI-optimized scalability.

Your Frontline Defense against AI-Fueled Web-attacks

The VMware Avi WAF is a distributed web application security solution leveraging closed-loop analytics and AI behavioral learning. It delivers an elastic solution unifying WAF, DDoS protection, rate limiting, encryption, and bot management to easily simplify policy customization. The platform actively blocks OWASP CRS exploits and ensures strict PCI DSS, HIPAA, and GDPR compliance by combining allow-lists, signatures, and AI-assisted positive-security models. Finally, its virtual patching capabilities instantly shield newly discovered, AI-fueled vulnerabilities, eliminating the race against exploits before developers can deploy permanent code fixes.

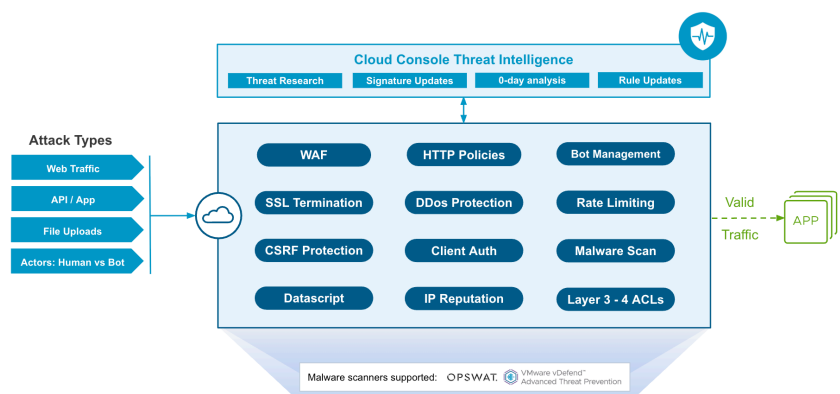


Figure 1: Application Security/WAF Comprehensive Security Stack and Insights

Frontier AI has turbocharged cyberattacks, launching complex exploits at speeds traditional patching cannot match. To protect VCF workloads across VMs and containers, Avi delivers an instant, full-stack defense. By combining AI-assisted behavioral learning to block AI-fueled attacks with instant virtual patching to neutralize active OWASP threats, Avi shields your applications inline without latency. This elastic, scale-out architecture easily absorbs high-volume attacks without degrading performance.

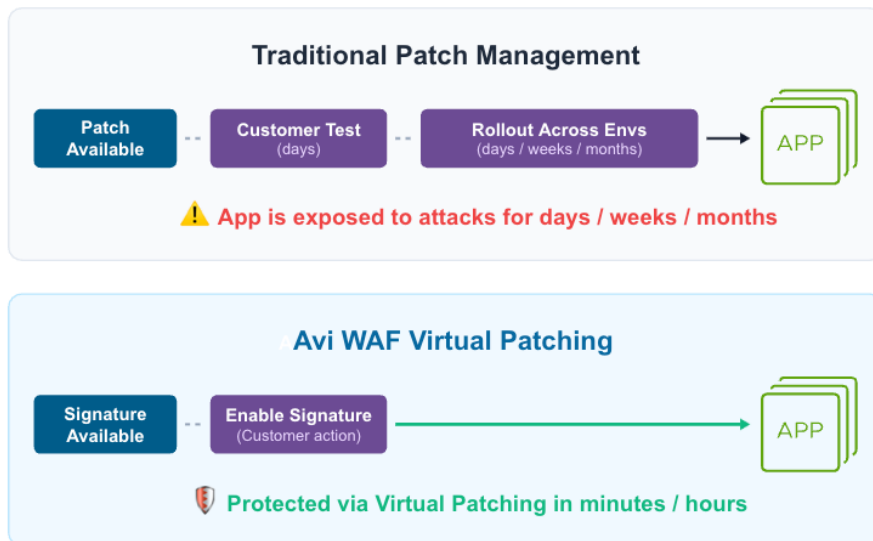


Figure 2: Avi's Virtual Patching

Avi's WAF gives administrators end-to-end security insights and analytics on performance, end-user interactions and security events in a single dashboard (Avi App Analytics) for actionable insights on security intelligence and enforcement. With Avi Cloud Console, live threat updates including IP reputation, signatures and more are sourced from industry leading threat analysis companies and curated. 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. WAF analyzes the unvalidated traffic through the allow list engine, positive security model that validates known good behavior as applications and attack patterns are learned and lastly, 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.

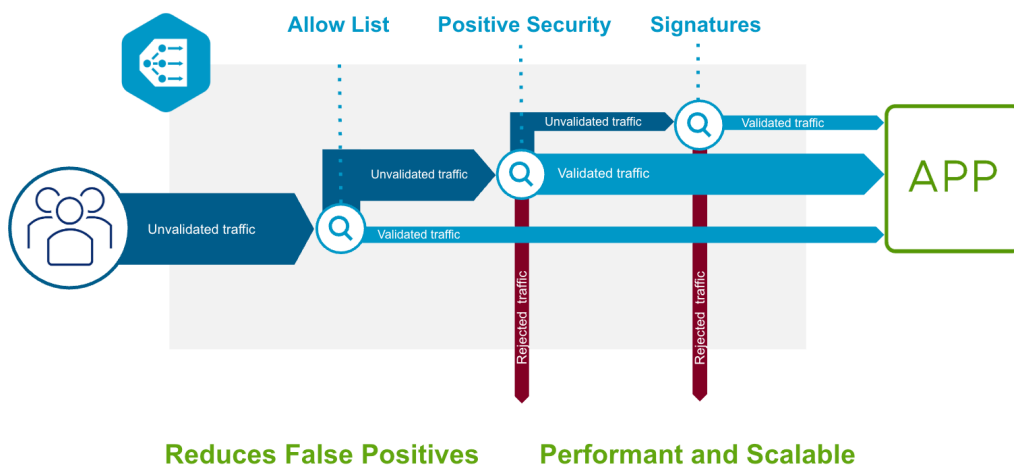


Figure 3: Avi WAF Security Pipeline Optimization

VMware® Avi™ Load Balancer Web Application Firewall (WAF)

Avi's bot management enables you to filter the bots that should be allowed to access the web assets and the bots that should be rate-limited or blocked.

See Figure 4.

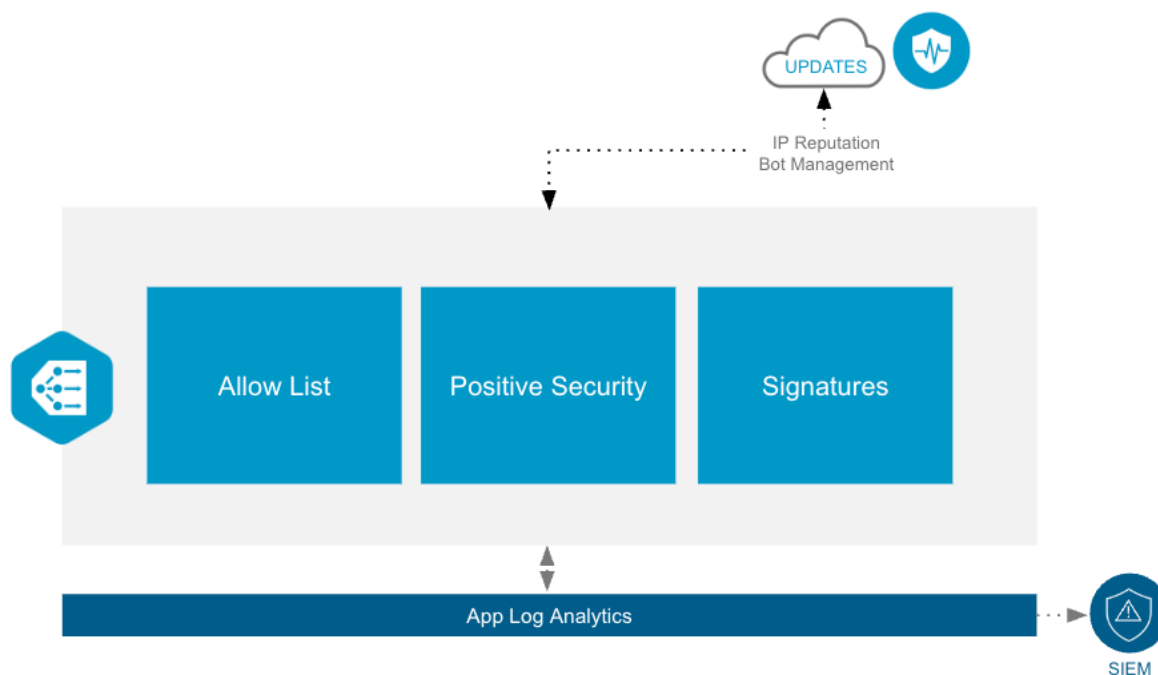


Figure 4 : Avi's Bot Management Pipeline

Bot management includes:

1. **Bot Detection** – The request goes through various checks to detect the bots.
2. **Bot Classification** – The bot is classified as human, good bot, bad bot, etc.
3. **Actions** – Defined to control the behavior of classified bots (rate limit, allow, close connection, end custom response, etc.).

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.
- **Instant Virtual Patching:** Protect web applications from AI-fueled web attacks with shorter patch window.
- **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

- **Allow List 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).
- **Application Rules** protect against known exploits in 3rd party, open source or closed source applications. Our database tracks over 5000 applications with 15k+ rules. Automatic updates ensure that your applications are always protected.
- **Automated threat updates.** Sourced from industry leading threat analysis companies Avi Cloud Console continuously updates the WAF threat 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 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.
- **Bot Management** to detect bot traffic, determine its intent, and mitigate bad bots to optimize customer experience, protect digital assets, and prevent online fraud. Bot management is available today as tech preview/beta version only.