SOLUTION BRIEF

CHALLENGES

- Web application attacks are on the rise, but web application security is lagging.
- Regulations and compliance requirements like GDPR, PCI DSS, HIPAA are increasingly common.
- Traditional web application firewalls (WAF) and web security solutions don't provide the compliance, scalability, or cost effectiveness that companies need.

SOLUTION

- SSL/TLS encryption, L3-7 ACLs that include both IP-port and URI based security rules, and rate limiting per app or per tenant.
- Avi's iWAF checks if all your security certifications are up-to-date, detects DDoS attacks and provides mitigation.
- Avi's iWAF helps protect against OWASP Core Rule Set (CRS) attacks and common signature-based vulnerabilities such as SQL injection and Cross-site Scripting (XSS).

BENEFITS

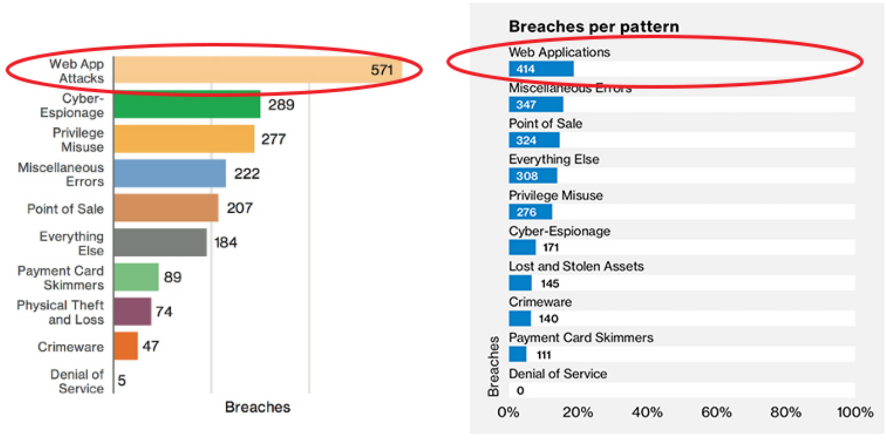
Avi's iWAF offers:

- Simplicity – from plug-and-play automation to simplified, configurable rules that are point-and-click.
- Visibility – detection of attacks, and security rules (OWASP CRS) that deflect those attacks.
- Elasticity – scalability to ensure robust performance regardless of traffic, while remaining secure.

Achieving Security and Compliance using Avi Vantage

THE STATE OF WEB APPLICATION SECURITY

Security breaches are on the rise. Verizon Data Breach Investigations in 2017 and 2018[1] (see Figure 1) show that web application attacks are the most prevalent breaches, but web application security—especially as web applications are increasingly deployed outside of traditional on-premise environments—is lagging.



Breach: An incident that results in the confirmed disclosure—not just potential disclosure—of data to an unauthorized party

Figure 1: Web application attacks rank #1 for security breaches in 2017 (left) and 2018 (right)

According to the Open Web Application Security Project (OWASP), many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and personal information. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. The ranking for "sensitive data exposure" among OWASP Top 10 threats has also risen from #6 in 2013 to #3 in 2017 (see Figure 2).

As a result, compliance requirements and regulations are increasingly reinforcing web application security. We will discuss the EU data privacy law General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS) and the industry specific rule Health Insurance Portability and Accountability Act (HIPAA).

[1] "Verizon 2018 Data Breach Investigations Report", https://www.verizonenterprise.com/verizon-insights-lab/dbir/

GDPR Compliance

GDPR focuses on data protection of personally identifiable information (PII). This mandate compels companies to apply the same level of protection for data such as an individual IP addresses or cookie data as they do for PII in compliance with IT policy.

At a high level, Avi Networks can help achieve GDPR compliance from three aspects:

- Data access: authentication using certificates, HTTP, and RBAC for sensitive data
- Datasecurity: SSL, audit trail with log search, and taps, IDS, IPS for further analysis
- Application security: protection using WAF, isolation with multi-tenancy at the data plane, and multi-cloud protection

PCI Compliance

PCI DSS is an established set of security measures and best practices that organizations must follow if they accept and handle cardholder data online. This standard encompasses network security, data protection, data encryption, system security, access control, ongoing monitoring and testing, and security policy development.

An organization can become PCI compliant by satisfying the requirements in Section 6.6, with either an independent code review or a WAF. Avi's recommendation is to implement a WAF with enhanced security features.

- Built in security policy looking for OWASP Top 10 threats and more to actively protect web applications
- Scanning outgoing responses that could contain sensitive data like credit cards and blocking them
- Automatic encryption and decryption of any traffic passing through its load balancer

HIPAA Compliance

HIPAA addresses the security and privacy of electronic protected health information (ePHI) and security concerns associated with the electronic transmission of health information. Audit trails can provide documented proof that your organization is conducting ongoing web application security assessments and monitor audits for HIPAA compliance.

Avi helps achieve HIPAA compliance with the following features built in the Avi Vantage Platform.

- Intelligent Web Application Firewall (iWAF)
- L3-L7 security rules including ACLs, rate limiting, DNS and DDoS protection
- URL filtering to prevent unauthorized access
- SSL/TLS for traffic encryption

Application Security Overview

Avi provides a comprehensive security stack (see Figure 2) that includes SSL/TLS encryption, L3-7 ACLs that include both IP-port and uniform resource identifier (URI) based security rules, and rate limiting per app or per tenant. Deep security insights provide real-time monitoring and overall health score for your applications. For example, Avi checks if all your security certifications are up-to-date, detects DDoS attacks, and provides mitigation.

Avi protects mission critical applications across any environment – on-prem data centers, private and public cloud. Avi Intelligent Web Application Firewall iWAF helps protect against OWASP Core Rule Set (CRS) attacks and common signaturebased vulnerabilities such as SQL injection and Cross-site Scripting (XSS).

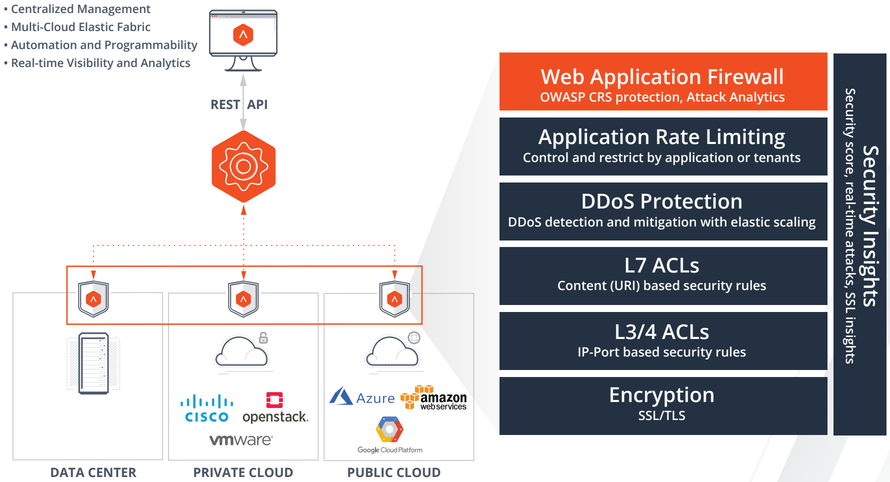

• Centralized Management
• Multi-Cloud Elastic Fabric
• Automation and Programmability
• Real-time Visibility and Analytics
REST API
DATA CENTER
cisco
openstack.
vmware
PRIVATE CLOUD
Azure
amazon webservices
Google Cloud Platform
PUBLIC CLOUD
Web Application Firewall
OWASP CRS protection, Attack Analytics
Application Rate Limiting
Control and restrict by application or tenants
DDoS Protection
DDoS detection and mitigation with elastic scaling
L7 ACLs
Content (URI) based security rules
L3/4 ACLs
IP-Port based security rules
Encryption
SSL/TLS
Security Insights
Security score, real-time attacks, SSL insights

Figure 2: Avi Security Overview