WHITE PAPER:
November 2024

Secure Your Web Applications and Achieve Compliance

vmware by Broadcom

Table of Contents

ABOUT THIS DOCUMENT

This white paper details the increasing risks that web application attacks (ranked #1 in security breaches) pose. Traditional web application firewalls (WAF) not only fail to comply with requirements like GDPR, PCI DSS, HIPAA, but also lack the scalability and cost effectiveness that companies need. VMware® Avi™ Load Balancer's WAF and its entire stack of security features provide unparalleled simplicity, visibility, and auto scaling capabilities to withstand threats.

"I believe there is no valid reason to provision a web application on the internet without a WAF. This is especially important to us since Swisslos needs to be compliant with industry regulations & certifications."

Joris Vuffray,
Head of Network &
System Management,
Swisslos

The State of Web Application Security

Security breaches are on the rise. Verizon Data Breach Investigations in 2023 and 2024[1] (see Figure 1) show that web applications are the top action vectors in breaches, but web application security—especially as web applications are increasingly deployed outside of traditional on-premise environments—is lagging.

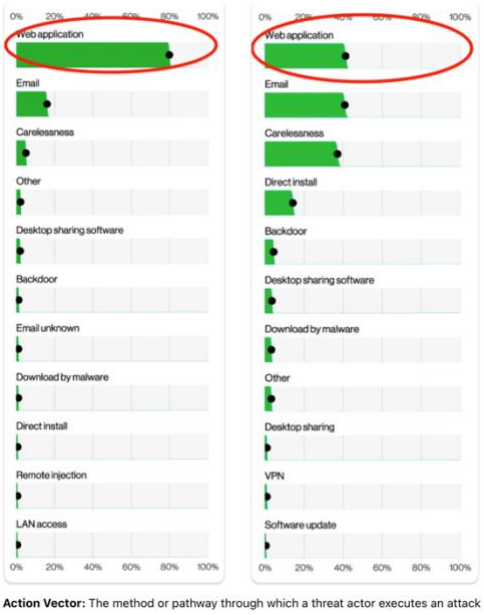

Figure 1: Web application attacks rank #1 as action vectors for security breaches in 2023 (left) and 2024 (right)

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.

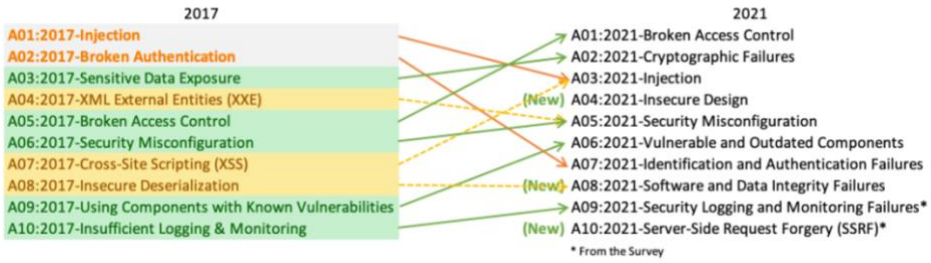

Figure 2: The Ten Most Critical Web Application Security Risks

[1] "Verizon 2023 Data Breach Investigations Report", "Verizon 2024 Data Breach Investigations Report"

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

PCI Compliance

The Payment Card Industry Data Security Standard (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.

With the release of PCI DSS Version 4.0, the requirements for securing web-facing applications have become more stringent. Requirement 6.4.2 mandates that organizations deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks. This means that, as of March 31, 2025, deploying a Web Application Firewall (WAF) will no longer be optional but a mandatory requirement for PCI merchants.

Avi's recommendation is to implement a WAF with enhanced security features. A few things to highlight are:

- Built-in security policies that actively protect web applications by looking for OWASP Top 10 threats and more.
- Scanning outgoing responses to detect and block sensitive data like credit card numbers.
- Automatic encryption and decryption of any traffic passing through its load balancer.

Implementing a robust WAF not only ensures compliance with PCI DSS 4.0 but also significantly enhances the overall security posture of your web applications.

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 such as names, addresses, and Social Security numbers. Ensuring that applications are protected, and that all access is in compliance with IT policy, is the best way to secure data.

At a high level, VMware Avi Load Balancer can help achieve GDPR compliance from three aspects:

1. Data access
    - Client authentication: using certificates
    - Client authentication: using HTTP basic authentication
    - Role-based access control (RBAC): controlling who has access to the sensitive data
2. Data security
    - SSL everywhere: encrypt everything
    - SSL visibility: decrypt SSL and send traffic to taps, IDS, IPS for further analysis.
    - Analytics and visualization: log search (audit trail), client insights and security health score
3. Application security
    - Application protection: using web application firewall (WAF)
    - Application isolation: multi-tenancy at the data plane
    - Multi-cloud: consistent protection across all environments.

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. Web servers, database servers and often the applications themselves have a logging function that creates audit trails for tracking who accessed information and when. These trails provide the details necessary for system monitoring and troubleshooting and are often used to investigate attacks against web applications. Audit trails can also assist with and provide documented proof that your organization is conducting ongoing web application security assessments and audits for HIPAA compliance.

Avi Load Balancer helps achieve HIPAA compliance with the following features.

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

Modern Architecture for Application Security

Homogenous IT environments are a thing of the past; today, applications within one company may be deployed over a combination of bare metal systems, VMs, containers, or a public cloud, so should change its security policies. Avi Load Balancer is built on a modern distributed architecture (see Figure 3) that separates the control plane from the data plane. Avi supports both traditional and modern use cases in a scalable, high-performing, and automated way.

Load balancers occupy a prime location - inline between users and applications. Avi is the first solution to take advantage of this location privilege to deliver rich analytics and visibility to help ensure that your web applications are secure and compliant.

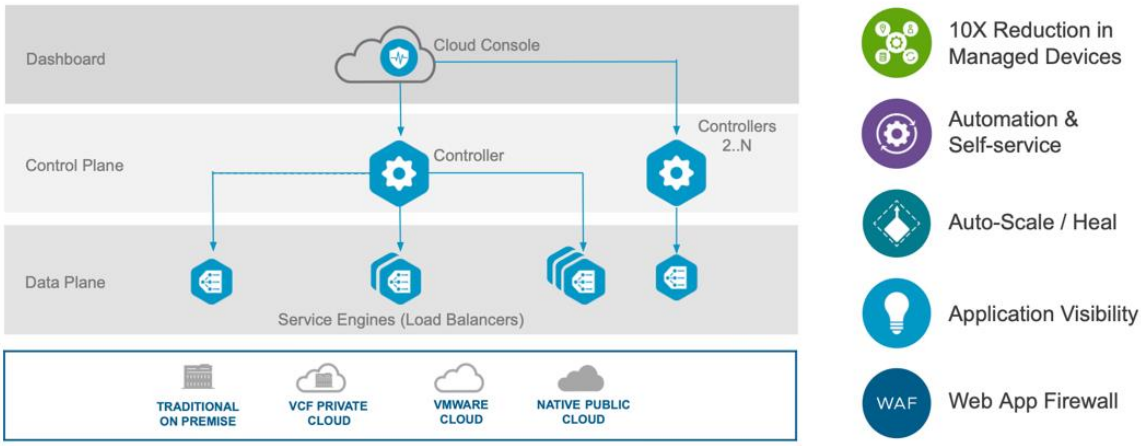

Figure 3: NSX Advanced Load Balancer Architecture

Application Security Overview

Avi Load Balancer provides a comprehensive security stack (see Figure 4) 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 WAF helps protect against common web application attacks, including SQL Injection and Cross-site Scripting (XSS), by implementing the OWASP Core Rule Set (CRS).

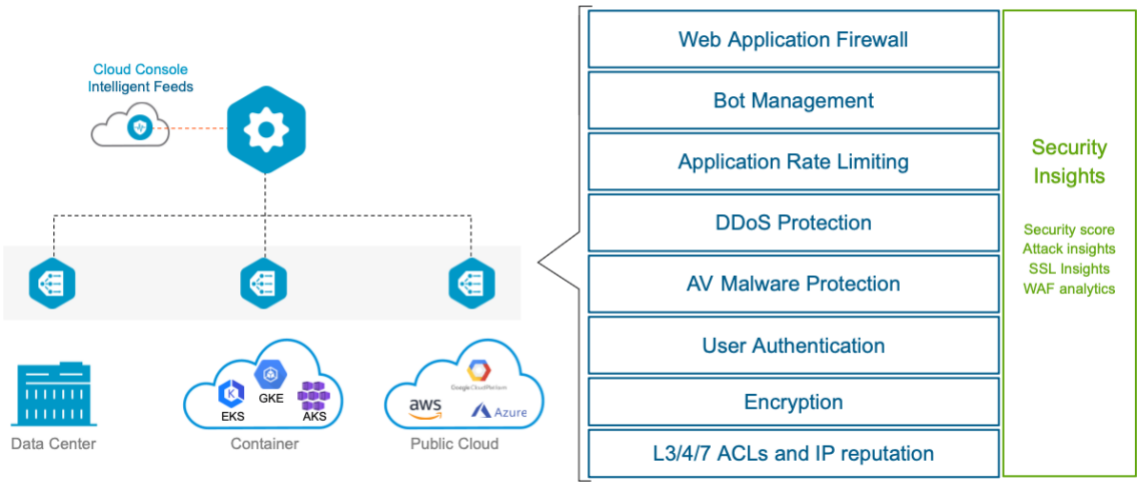

Figure 4: Avi Security Overview

WAF Delivers Simple, Scalable and Intelligent Web Security

Avi Load Balancer's WAF delivers high-performance web application security with point-and-click simplicity. It enables customized policy configurations and helps achieve compliances like GDPR, PCI DSS and HIPAA. It simplifies security rules, minimizes false positives with advanced analytics, and protects applications from DDoS attacks and OWASP Top 10 threats with real-time insights.

Avi WAF allows businesses to operate securely without sacrificing performance or scalability—while reducing operating costs—even during peak times. Swiss lottery company Swisslos, with unpredictable load patterns that increase when the jackpot amount rises, is now able to scale in real time and can securely support web traffic with WAF, a software-defined solution. In the past, when experiencing peak loads, Swisslos would turn off its appliance-based WAF, sacrificing security in order to achieve performance objectives.

As a completely software-defined solution, Avi WAF scales with the business without sacrificing performance. Companies can scale application services quickly with existing WAF software without having to deploy or configure costly physical appliances, as is common with hardware-based WAF products.

WAF Simplifies Security Configuration to Protect Business

Avi WAF simplifies security configuration, offering predefined built-in, yet still configurable, rules. Unlike traditional WAFs, where so much time is spent on configuring complex rule sets instead of keeping businesses safe, WAF's simplified rule setup (see Figure 5) allows organizations to secure applications quickly and confidently.

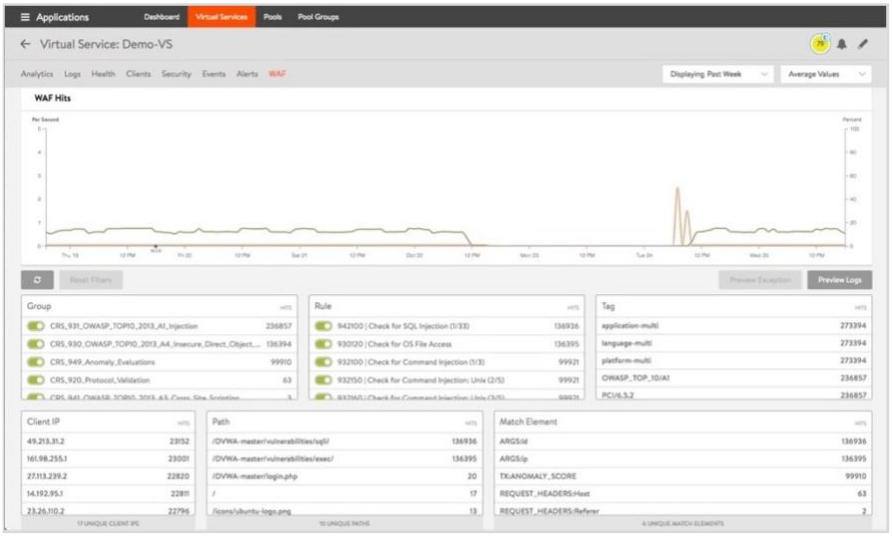

Figure 5: Simple Point-and-Click OWASP CRS Security Rules

Rules and policy groups are also configurable, allowing security teams and application teams to tune rules, such as adding exceptions, in real time to meet their needs.

WAF Provides Real-Time Insight into Application Security

Traditional WAFs are a "black box," offering no visibility into how rules are working or how they are impacting performance. WAF provides real-time insight into application traffic, user experiences, the security and threat landscape, and application performance. This allows businesses to identify and protect against the most sophisticated attacks while ensuring that users have the access and performance they expect.

With the GDPR's 72-hour breach notification rule, having insight into threats within your network traffic is critical. Most breaches remain undetected for many months or even years. It's important to have visibility into the state of security (see Figure 6) to secure your web applications.

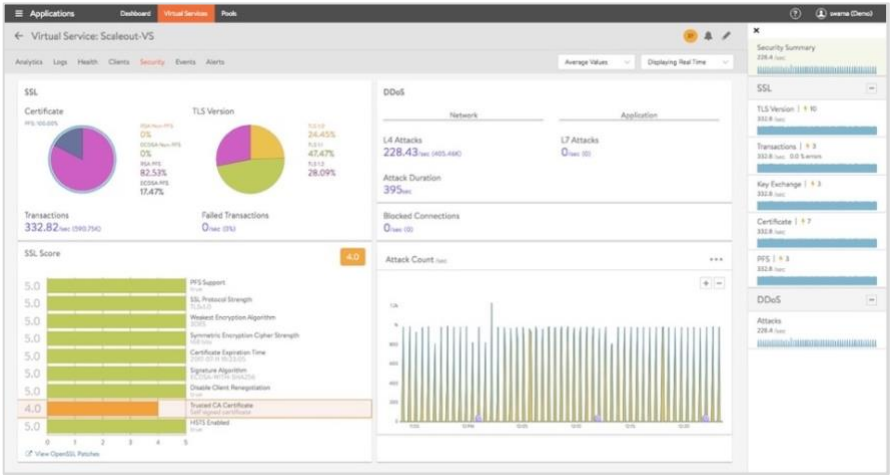

Figure 6: Avi Analytics Provides Security Insights

Analytics from WAF ties in closely with the simplified rules configuration, enabling an administrator to tune rules in real time based on gathered intelligence. This real-time analytics-based tuning allows the business to better secure web applications against attacks in the moment.

Conclusion

As web attacks increase and as businesses change their IT infrastructures, traditional web application firewalls and web security solutions don't provide the compliance, scalability, or cost effectiveness that companies need. With the increasing level of regulation and compliance requirements, businesses need solutions to keep web applications secure now and in the future, even as attack vectors change and grow more sophisticated.

Avi security offers businesses:

- **Simplicity**, from plug-and-play automation with traditional and modern IT architecture to simplified, configurable rules that allow businesses to get web applications up and running quickly.
- **Visibility** into the types of attacks hitting the system, as well as how defined rules are deflecting those attacks.
- **Elasticity**, providing scalability to ensure that web applications are performing as expected, regardless of traffic, while remaining secure.

Avi provides both protection and performance, allowing companies to scale and grow at the speed of business.

Item No: vmw-bc-wp-tech-temp-uslet-word-2024 1/24