WHITE PAPER: **September 2024**

# Protecting Applications with VMware® Avi™ Load Balancer

vmware® by Broadcom

## Table of Contents

# Overview of VMware Avi Load Balancer Application Security

## Introduction

The cybersecurity threat landscape that organizations face is complex and constantly changing. Businesses are challenged with protecting their applications and data in today's IT threat landscape. They need to protect their applications in the current multi-cloud and containerized environments. Threats are evolving to become more sophisticated, attacking the applications, their APIs and new platforms. Cybercriminals and state-backed actors are actively targeting businesses, the public sector, all layers of government, and critical infrastructure. They do this to cause disruption, steal personally sensitive information or intellectual property, or get financial gain via ransomware.

Defending an organization against the multiple threats they face requires a multilayered approach that includes defenses at numerous entry points that cybercriminals target to bypass protections. Protection requires a multi-layered approach that incorporates multiple technologies. In this white paper, we'll outline, without diving deeply into the technical details, how the cybersecurity solutions provided by VMware Avi Load Balancer enable organizations to secure their modern, complex environments.

## Executive Summary

The VMware Avi Load Balancer delivers a stack of protection technologies that defend against different attack vectors that cyberattacks use. The tools work in harmony to provide an overall level of protection greater than what they would provide individually.

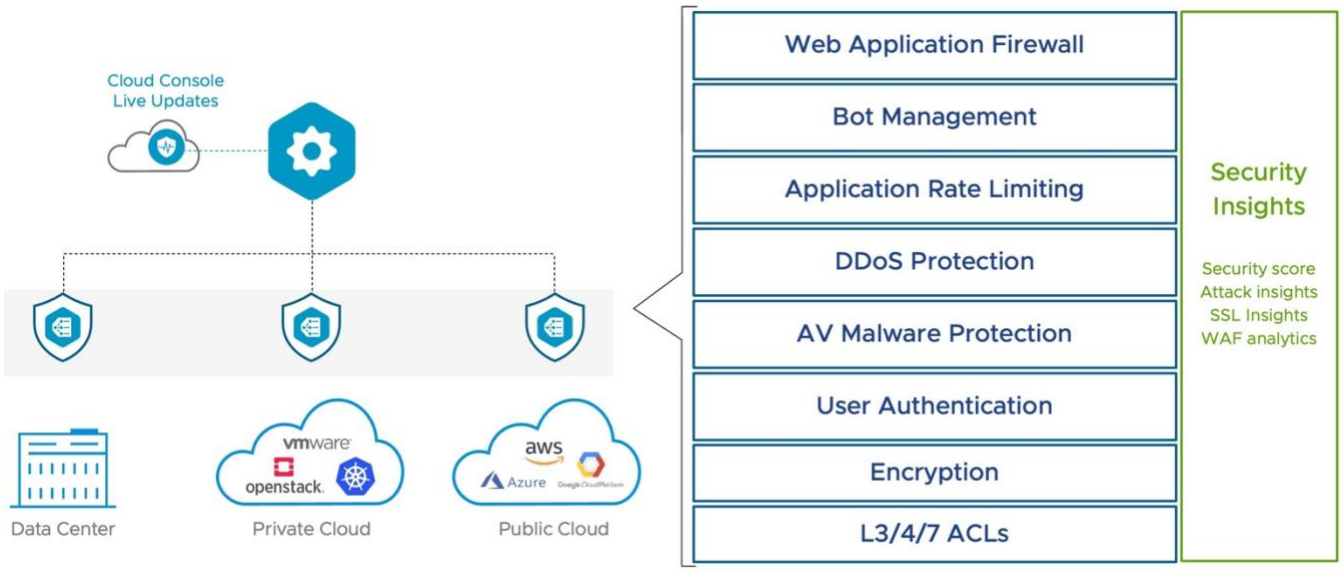


Figure 1: Avi Load Balancer Application Security Solution High-Level Architecture

C-suite and other executives in organizations of all sizes and across all sectors must ensure that cybersecurity is a front-and-center consideration of their IT team. The risk from cyberattacks such as ransomware or data breaches can be existential. Some organizations never fully recover from a high-profile cyber attack's technical impacts and reputational damage.

Cybersecurity protection requires a multilayered approach. Protection technologies need to be deployed at the appropriate layer to be effective. These technologies need to integrate well to present the big picture to cybersecurity teams. But at the same time, this multilayered approach shouldn't introduce complexity that increases the likelihood of a threat getting missed.

Avi Load Balancer's cybersecurity solution provides this multilayered but joined-up protection today and delivers automatic updates to continue to protect your organization as the threat landscape changes. The components that give each layer of

protection add up to provide a cybersecurity protection suite greater than the sum of its parts. All delivered with the security of knowing that Avi Load Balancer is part of an industry-leading provider as part of the VMware family.

While the technical and procedural details of cybersecurity defenses should reside with the CISO (Chief Information Security Officer) or the head of IT, other executives need to be aware of what protections are required and should ensure that they are in place by asking pertinent questions of their technical colleagues.

The sections below outline how the VMware Avi Load Balancer Application Security Solution delivers the protection organizations need in six core areas without introducing unnecessary complexity due to integration between toolsets.

Security should always be a multi-layered and multi-targeted process. The solutions discussed here complement the other VMware security capabilities within VMware's cloud strategies such as VMware Cloud Foundation and VMware vDefend lateral security capabilities. The six technologies discussed in the solution within the Avi Load Balancer are:

**API protection** - Application Programming Interfaces (APIs) deliver connectivity between IT systems, enabling integration and data flows. They are a prime target for cybercriminals, so organizations must protect APIs. Gartner predicts that by the end of 2022, application programming interface (API) attacks will become the most-frequent attack vector causing data breaches for enterprise web applications.

**Web application firewall (WAF)** - A WAF provides security functionality for applications that interact with end users via web protocols and browsers. WAFs sit between the users and the backend servers to screen requests and traffic for malicious or suspicious activity. They complement but do not replace other network security solutions, such as network firewalls and intrusion detection systems (IDS).

**Bot identification and management** - Studies show that nearly 40% of internet traffic originates from bot activity rather than from humans accessing apps and sites from their devices. Some of this bot activity is required for the health of sites and for search discoverability. But over a fifth of bot activity is classed as bad and should be blocked by organizations. In either case, all bot activity needs to be monitored and managed. Failure to do so has operational risks, as the bot activity can have detrimental impacts on the performance of online sites and applications when staff, clients, and customers need to access websites.

**Network data encryption** - Encrypting data when it moves between servers and endpoints on the network is fundamental to all cybersecurity strategies. Any data transmitted without encryption is vulnerable to interception and open to eavesdroppers. The Transport Layer Security (TLS) protocol version 1.3 should be used for encrypting network traffic. This has superseded the Secure Sockets Layer (SSL) protocol, although the term SSL is still often used when discussing network encryption. Ensure that your cybersecurity teams are using TLS. Preferably TLS 1.3, but in some instances TLS 1.2 is required (Microsoft Exchange Server still uses TLS 1.2 at the time of writing in late 2022).

**Denial of service attack protection** - Denial of service attacks are sadly a constant threat to organizations of all sizes. Distributed Denial of Service (DDoS) attacks are the most common type, and they are used to take web applications offline or to cover other cyberattack activity, such as ransomware deployment. DDoS protection needs to be provided via a combination of network provider services or dedicated DDoS protection services such as Cloudflare, Akamai, Imperva, or others, and local on-premise monitoring, alerting, and response measures like those provided by Avi Load Balancer.

**Authentication** - It is essential that it's always known who is connecting to your IT systems, that they are authorized to do so, and are using a secure authentication method. Avi Load Balancer provides an authentication service that supports several authentication technologies, allowing for connection authentication and single sign-on where appropriate.

## Overview of the Protection Solutions Delivered

The six sections below outline core cybersecurity protections delivered by Avi Load Balancer. Figure 2 shows the technology stack that protects applications and users from threats that arrive via web traffic, API/App, file uploads, and via sophisticated identification to separate connections made by humans and bots.

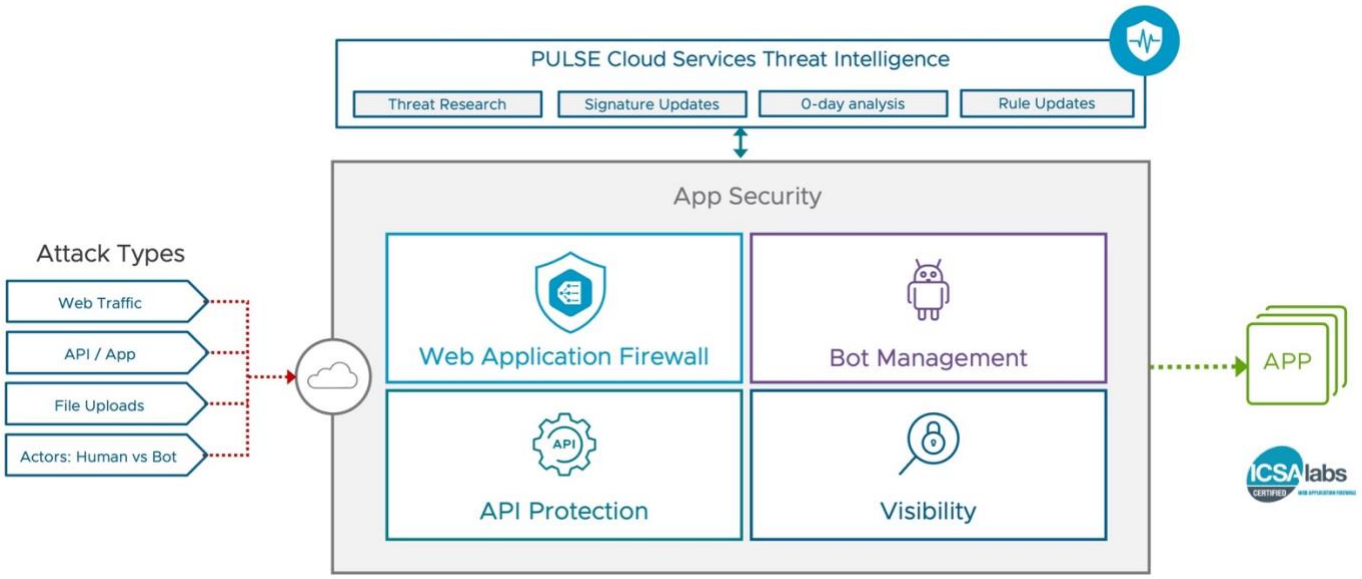


Figure 2: Avi Load Balancer Application Security Solution

### Comprehensive API Protection

Most end-user computer interactions occur via the use of applications. These applications can be web-based in a browser, native applications running on a PC or mobile device, or hybrid applications that are essentially a web view with a native wrapper. Almost all business apps will communicate with backend server infrastructure that provides core functionality via database, content delivery, and application servers.

In current deployments, the supporting infrastructure for both the backend servers and applications will run on on-premise hardware, virtual servers (on-premise or in the cloud), as fully native cloud instances, and increasingly as micro-services and applications that run in containers.

Because applications of all types play such an essential role in the modern business landscape, they are a tempting target for cybercriminals looking to exploit vulnerabilities to steal data or gain access to deploy malware and ongoing advanced persistent threats (APT).

The Verizon Data Breach Investigation Report 2022 highlighted that attacks targeting applications via API vulnerabilities are one of the fastest-growing attack vectors used by cybercriminals.

APIs play a crucial role in the modern interconnected world and provide the communication pathways that different systems use to interact. APIs underpin the digital platforms that enable computer systems to power many things we now take for granted, including transport systems and healthcare, and provide the tools driving digital transformation in many organizations.

The widespread use of APIs has increased the surface attackers can probe for weaknesses. Plus, the importance of the data carried via APIs has increased the rewards attackers can gain if they find a vulnerability. The number of API vulnerabilities discovered has risen markedly in recent years. Highlighting how this attack vector is now of vital importance and one that needs focus.

Avi Load Balancer has advanced cybersecurity functionality to protect applications and their APIs irrespective of whether they are running on-premise in private cloud deployments, running via a public cloud provider, via virtual machines, or in containers hosted wherever containerization solutions get deployed.

The API protection solution detects threats with API communications between systems via rich layer-7 content inspection technologies, including encrypted traffic (as all traffic should be when passing between systems). The Avi Load Balancer solution uses a powerful inspection engine to examine API traffic to determine whether the content is valid. It uses pattern matching and robust comparison checking for known vulnerabilities such as buffer overflows, SQL injection, and many more. Figure 3 shows the protections the solution provides for API security.

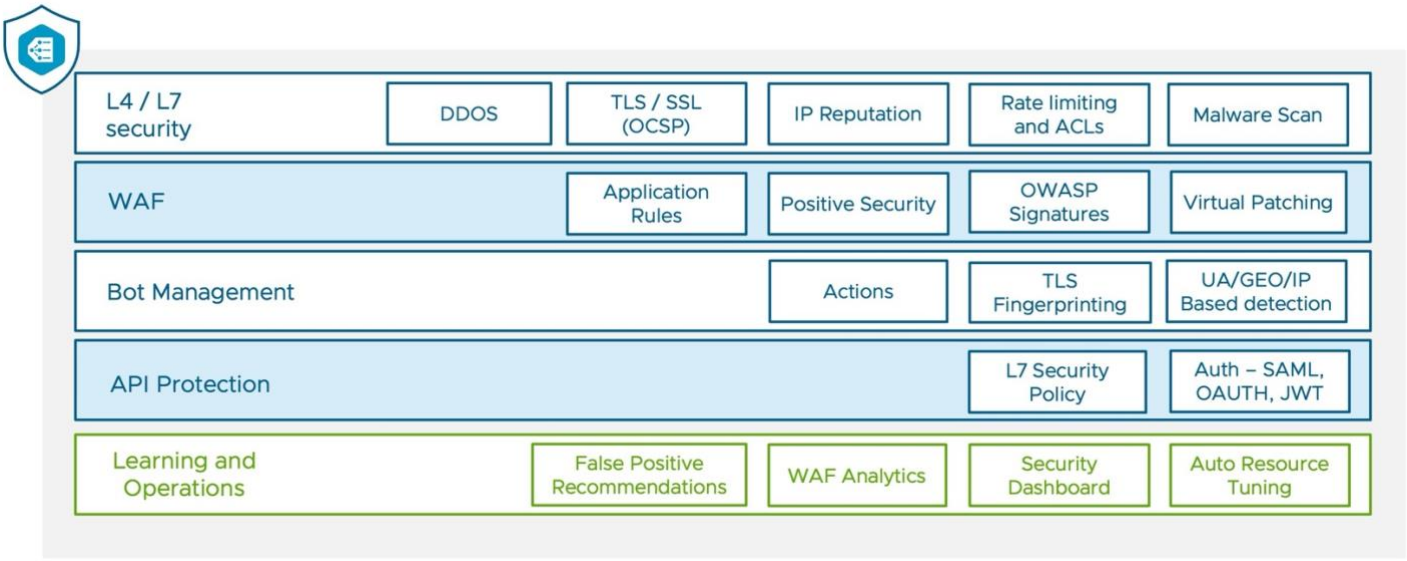


Figure 3: Avi Load Balancer Protections

Protection for applications deployed via microservices and managed via Kubernetes in containerized clusters, and the APIs used to access these apps, are now a significant part of the application deployment landscape. The Avi Load Balancer Kubernetes Ingress Services Solution provides a centrally orchestrated, elastic proxy services fabric with dynamic load balancing, service discovery, security, micro-segmentation, and analytics for containerized applications running in Kubernetes environments.

## Context-Aware Web Application Firewall

Protecting applications from the ever-changing threat landscape is a central part of all the cybersecurity protections that organizations should implement. A WAF works alongside other network protection solutions, such as traditional network firewall security devices. Network firewalls typically don't have visibility across the OSI network stack. For example, they usually can't inspect HTTPS traffic to look for threats.

WAFs operate at upper network layers such as the Application layer (L7), in addition to the Network (L3) and Transport (L4) layers, and are placed between border firewalls and backend application servers. They can decrypt HTTPS traffic to inspect the data packets at this logical position on the network. A WAF can deny application server access to any traffic deemed a threat using rules, intelligence engines, lists of known attack vectors, and anomaly detection.

VMware Avi Load Balancer WAF uses a multifaceted approach and set of protections to deliver robust security that uses the WAF and the other cybersecurity protections outlined here to deliver enhanced cybersecurity for all organizations. Figure 4 provides an overview of the Avi Load Balancer WAF components.

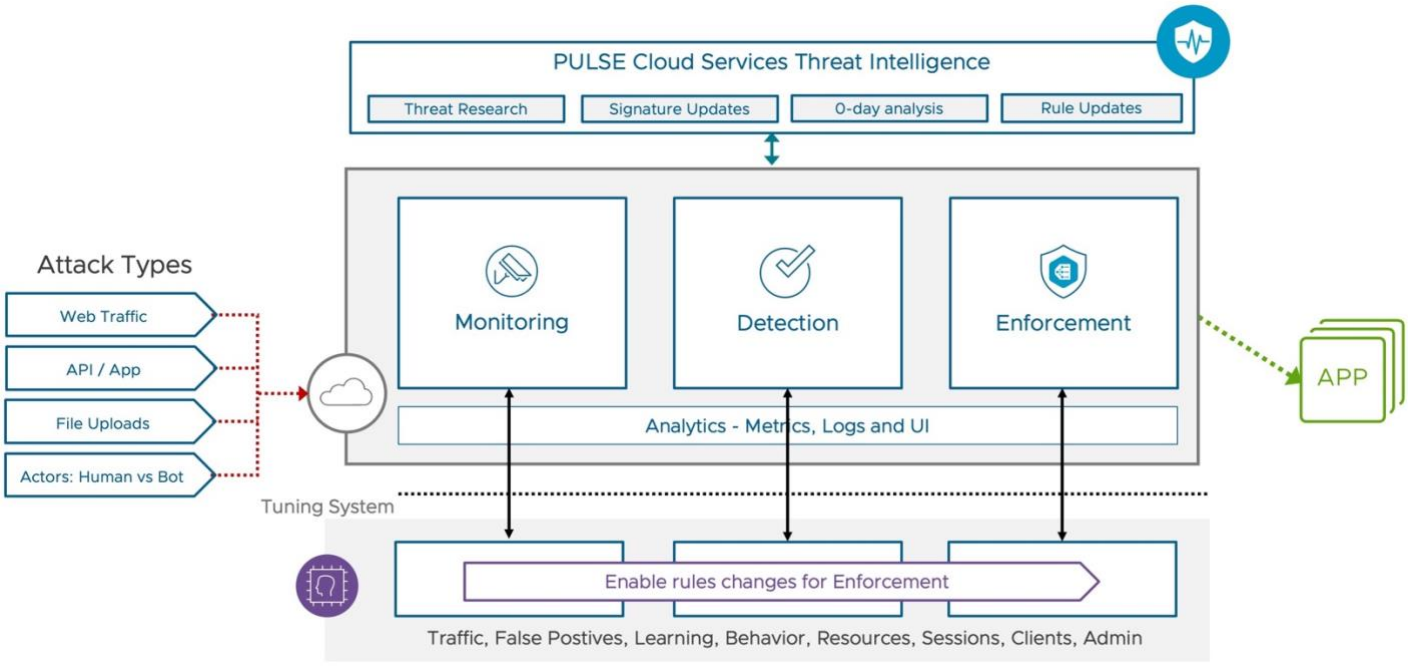


Figure 4: Avi Load Balancer WAF Security

The security protections delivered by the WAF fall into three categories.

**Core Security** - The core security category delivers the following cybersecurity protection technologies.

- OWASP Top 10 attack protection, including HTTP validation, injection protection, 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 enables users to create custom policies quickly and efficiently.
- RBAC (Role Based Access Control) support to control write access to WAF profiles and policies, plus read access to applications, pools, and clouds.

**Threat Detection** - Delivers rules and responses triggered by detected threats or anomalies.

- 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.
- Signature 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 OWASP ModSecurity Core Rule Set (CRS).
- Application Rules protect against known exploits in 3rd party, open-source, or closed-source applications — the 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 Load Balancer Pulse Services continuously updates the WAF thread database with IP reputation, signatures, and more, protecting web applications from common and new vulnerabilities.

**Application Protection** - Specific rules and deployment configurations to protect individual applications in the best way possible.

- Positive Security Model rules define allowed application behavior and can be created manually or automatically by the learning engine through sampling traffic.
- 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. More on bot protection in the next section.

The Avi Load Balancer WAF delivers modern application protection with point-and-click simplicity. It is designed to provide protection from threats while also being easy to deploy and manage. To facilitate this, the WAF can learn application behaviors and provide tailored security policies without overburdening the security operations team.

In addition to the robust security protection, the WAF also helps deliver compliance with global and regional regulations and industry standards such as GDPR, CCPA, HIPAA, and PCI DSS. Avi Load Balancer WAF implements protection against the most prevalent attack methods, such as those included in the OWASP Top 10 and others, via industry-standard rulesets like the OWASP ModSecurity Core Ruleset.

## Bot Identification and Management

Recent studies show that up to 40% of internet website traffic originates from bot activity. Depending on the website's purpose, this bot traffic could be good (for example, search engine crawlers) or bad (website scrapers). Of the 40% of traffic typically created by bots, approximately 15% delivers welcome functionality - this traffic comes from good bots. However, the other 25% comes from bad bots undertaking activities that most organizations will want to prevent.

The goal of Avi Load Balancer cybersecurity when it comes to bots is to firstly perform effective intelligent identification between human-generated traffic and that from bots. Multiple techniques get used in making this distinction. Once a determination is made and bot traffic identified, the Avi Load Balancer solutions allow each organization to decide how to handle it based on their specific needs.

VMware Avi Load Balancer includes a management solution to deal with bot traffic. It uses an engine that has three core components. Figure 5 shows them:

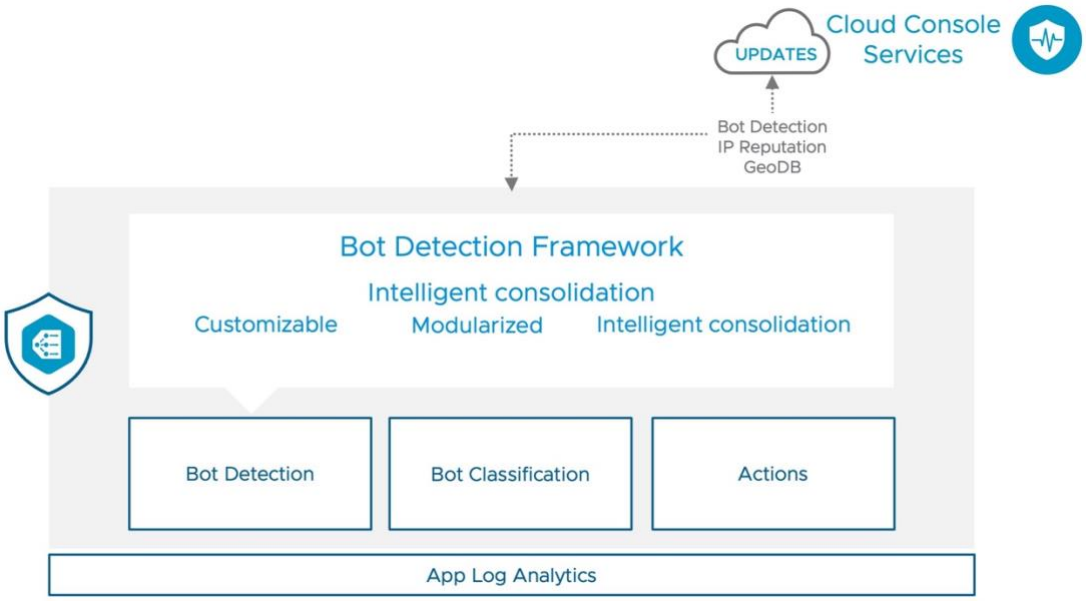


Figure 5: Avi Load Balancer
Vantage Bot Protection Engine Components

The bot protection builds on the solid core of the Avi Load Balancer WAF pipeline, which delivers web cybersecurity. The core components provide the following:

**Bot Detection** - The primary and most crucial step in bot protection. Various checks such as IP reputation, IP location, User-Agent ID, Origin Network (ASN), and others get used for this step. TLS fingerprinting that compares TLS information against that expected from a particular user agent is also used. Note that IP reputation and other data used in detection get updates via the Avi Load Balancer PULSE Cloud services and that a subscription to this is required to use Avi Load Balancer bot protection.

**Bot Classification** - The engine uses the information gathered and decision algorithms to determine if a particular connection is coming from a bot or a human. If a connection is from a bot, the engine classifies the bot type using a bot mapping policy. The classification types are Human, Good Bot, Bad Bot, Dangerous Bot, User Defined, and Unknown Client.

**Actions** - Business logic is used for each type of classification using HTTP policies, DataScript, or WAF rules. The choices available are: Allow, Close Connection, Rate Limit, and Send Custom Response.

To learn more about Avi Load Balancer bot management's technical details, visit the documentation page in the References section.

## Enhanced Encryption via TLS Offload

Encrypting data as it travels over a network (plus when at rest on server storage or devices) is essential. All the cybersecurity protections available are moot if encryption is not in place to protect data. Additionally, the provision of encryption for data needs to be transparent to end users. There should be no overhead that impacts the data transmission speed or its availability for use.

Protection for data moving over networks should use TLS encryption. TLS 1.3 is the latest version everyone should use as it is the most secure and has superseded previous versions of TLS and all SSL versions. It's still common to see SSL used when discussing network data encryption, but TLS should be what gets used to encrypt the data.

TLS processing, when done on application servers, can introduce a significant overhead. The servers need to decrypt incoming data traffic before processing it and then encrypt the outgoing traffic flowing to clients. This uses CPU and memory resources on the server, meaning it can serve fewer connections in a given period.

VMware Avi Load Balancer includes TLS offloading (née SSL offloading) that allows the encryption and decryption process to get offloaded from application servers. Using TLS offload via Avi Load Balancer enables applications to operate using strong encryption without having the performance overhead of handling TLS on backend servers. Traffic flowing between client devices and application servers is encrypted and decrypted as required, so that it remains secure and can be processed as quickly as possible.

The Avi Load Balancer TLS engine supports all modern security standards, such as TLS 1.3, RSA 2K key encryption, and advanced ECC encryption algorithms. Avi Load Balancer supports all modern key exchanges and certificate authorities. The Avi Load Balancer solution encrypts and stores TLS keys securely in a database, and they are never stored on a disk in clear text or transmitted across the network.

Avi Load Balancer' encryption engine also natively integrates with industry-leading hardware Security Modules (HSMs) for custom certificate management workflows, key storage, and secure TLS handshakes.

## DDoS Detection and Mitigation

DDoS attacks have been a threat to networks for a long time. In 2022 the number of DDoS attacks and the data they use is still increasing. The attack method is increasingly used to extort ransom payments from organizations. The cybercriminals attack a website, prevent legitimate access via their DDoS attack, and then demand a fee to terminate the attack. Protecting networks and applications from DDoS attacks is a crucial part of cybersecurity.

Due to its location on the network between users and applications, Avi Load Balancer is ideally placed to deliver focused DDoS protection against attacks such as SYN Flood and DNS Reflection attack types. Figure 6 provides an overview of DDoS protection at various network layers.

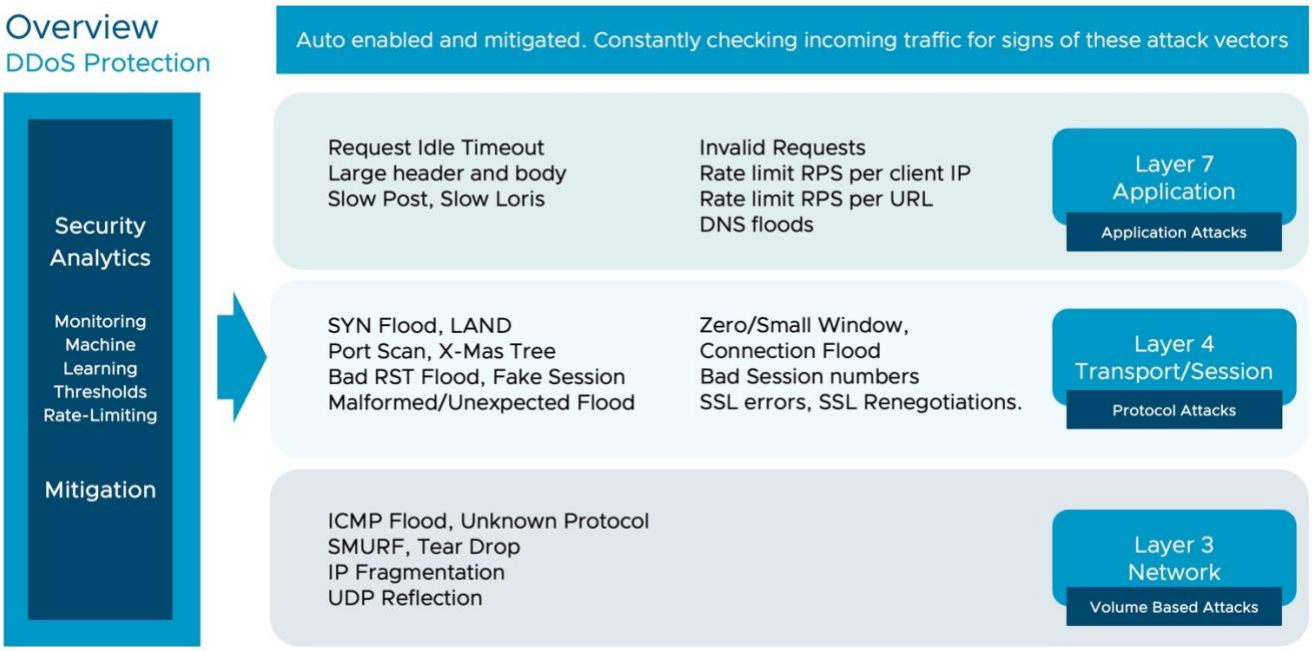


Figure 6: Avi Load Balancer DDoS protection mechanisms

There are many types of DDoS attacks, but they can be grouped into three broad categories -

- **Volumetric attacks** - These overwhelm the targeted website or application by generating lots of requests or sending lots of data. This uses all the bandwidth available to the hosting site and real user requests timeout. Volumetric attacks occur at the L3 network layer in the OSI model.
- **Protocol attacks** - Several types of protocol attacks get used for mounting DDoS attacks. They all work by sending an overwhelmingly large number of requests to a crucial protocol endpoint running on a server. They operate at both L3 and L4 of the OSI stack. Examples of protocol tack types include:
  - **SYN flood** - Ties up the attacked server via the TCP handshake protocol and causes timeouts.
  - **TCP reset** - Sends fake TCP reset commands to the attacked server causing it to drop connections with legitimate users.
  - **UDP flood** - UDP does not do handshaking when setting up connections. Attackers can therefore send UDP requests to targeted servers asking for connection on ports that may or may not exist. If the port doesn't exist, the server responds with an unreachable destination response. Sending many such requests overwhelms the server as it sends unreachable destination responses.
  - **ICMP (Smurf) attack** - Forged ICMP messages are sent to servers on the network with the return address forged to be the IP address of the server that the attackers want to target. When servers that get the ICMP request respond, they all send them to the attacked server and swamp it. A common malware attack method known as Smurf uses this DDoS attack method as part of its strategy.
  - **Reflected DNS attack** - Similar to an ICMP attack, but in this case, the forged return IP address is included in spoofed routes to DNS servers. The multiple requests to the DNS servers are all reflected back to the server the attackers are targeting.
  - **Reflected NTP attack** - The same as reflected DNS attacks but uses network time servers to send multiple requests to the attacked server.
- **Application attacks** - These DDoS attack methods target application and service functionality operating at Layer 7 (Application Layer) in the OSI stack. These are also known as HTTP flood attacks. Examples include:
  - **GET flood attack** - Requests to URLs providing an applications interface get continually sent to prevent requests from real users from getting processed.
  - **POST flood attack** - The mirror image of the GET flood attack. Rather than sending requests for data, the POST attack sends an overwhelming number of write requests to a server. Again, this prevents it from processing legitimate write requests.
  - **Low and Slow attacks -** These attack types slowly build over time to eventually overwhelm the server. They operate by not releasing the access slots allocated, and ultimately, the application server will be unable to serve any more access requests. Slowloris is an example of this type of attack, but given the slow nature of the build-up, Slowloris can also be a DoS that comes from a single attack source.

Avi Load Balancer protects against DDoS attacks by identifying threats, alerting admins, and automatically protecting against these attacks. Policies are available to order the dropping of any network traffic that falls outside predefined limits. The features available in the Avi Load Balancer platform to deliver comprehensive DDoS protection include TCP SYN Flooding Protection, HTTP DDoS Protection, URL filtering, Connection Rate Limiting per Client, Connection Rate Limiting per User Defined Clients, Limiting Max Throughput per virtual service, Limiting Max Concurrent Connections per virtual service, and by Limiting Max Concurrent Connections per Server.

Additionally, Avi Load Balancer' elastic application services enable on-demand autoscaling during an attack to give administrators time to work on mitigating the attack while maintaining the quality of service.

## Authentication

Authentication of incoming connection requests to web applications is an essential component of the overall cybersecurity protection chain. It's vital to make sure that requests are from valid sources. Avi Load Balancer provides an authentication service that supports several authentication technologies. Supported authentication methods for incoming requests from users or other applications are:

- **Basic** - Simple and widely used authentication mechanism in HTTP-based services or APIs. You can send HTTP requests with the authorization HTTP header that contains the word Basic followed by a space and a base 64-encoded string username:password pair.
- **LDAP** - LDAP is an extension of the basic authentication policy where the provided username and password get authenticated against the target LDAP server. Many standard LDAP servers can be used to authenticate virtual services on the Avi Load Balancer.
- **JWT** - JSON Web Tokens (JWT) are an open standard for securely transmitting information between nodes on the network. JWT uses a set of JSON objects tied together that are used over the web or between a client and a server to authenticate a connection request. They use private and public key verification.
- **SAML** - SAML is an XML-based markup language for exchanging authentication and authorization between an identity provider and a service provider. Avi Load Balancer supports several industry-leading identity provider services. SAML can be used to facilitate single sign-on where this is appropriate, and the security design allows it.
- **ADFS** - Microsoft Active Directory Federation Services (ADFS) is a common way to deliver authentication across on-premise and cloud-based deployments using Microsoft Active directory as the core LDAP-based authentication service in hybrid deployments. Avi Load Balancer supported ADFS as a SAML identity provider.
- **RBAC** - Modern applications often get deployed via many microservices that communicate across the network rather than as monolithic applications. Avi Load Balancer support RBAC to allow for granular control, management, and monitoring of distributed applications.

## References

Links to reports, data sources, and tools referred to in this white paper.

Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/

Gartner Predicts 2022: APIs Demand Improved Security and Management
https://www.gartner.com/en/documents/4009103

Webinar: Gartner API Security: Protect your APIs from Attacks and Data Breaches
https://www.gartner.com/en/webinars/4002323/api-security-protect-your-apis-from-attacks-and-data-breaches

ESG Trends in Modern Application Protection Infographic
https://www.esg-global.com/research/esg-infographic-trends-in-modern-application-protection

Statista: Distribution of bot and human web traffic worldwide from 2014 to 2021
https://www.statista.com/statistics/1264226/human-and-bot-web-traffic-share/

OWASP ModSecurity Core Ruleset
https://coreruleset.org

Avi Load Balancer BOT Management Documentation
https://docs.vmware.com/en/VMware-NSX-Advanced-Load-Balancer/30.1/Cloud-Console-Guide/GUID-B9D00777-AF00-4490-BB3F-3B159A41F0E5.html


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