VMware Cloud Web Security

vmware®

Cloud Web Security™

Introduction

VMware Cloud Web Security™ is a cloud-hosted service that protects users and infrastructure accessing SaaS and Internet applications from a changing threat landscape. The solution offers IT teams visibility and control, and ensures compliance, when users access SaaS applications. VMware Cloud Web Security is delivered through a global network of VMware edge points of presence (VMware Edge PoP™) to ensure optimal access to applications.

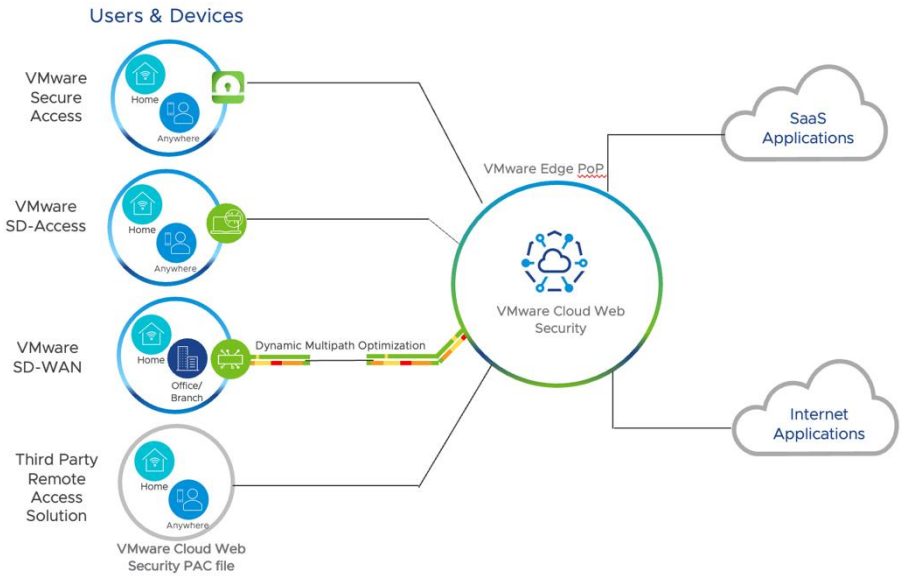

Figure 1: VMware Cloud Web Security protects user traffic accessing web applications.

VMware Cloud Web Security benefits

Agile security posture

VMware Cloud Web Security enables enterprise security teams to adapt to changing threat landscapes and business needs without leaving gaps in their security posture. The cloud-based solution takes advantage of up-to-date threat intelligence related to new virus signatures discovered or updates to website categorizations to help tighten attack surfaces. VMware Cloud Web Security removes the scale challenges seen with on-premises appliances as enterprises adopt an increasing number of SaaS and Internet applications. It offers actionable insights to tighten security posture.

Seamless security for the anywhere workforce

Users at branches, remote locations, at home, or on the move get optimal and secure direct access to Internet and SaaS applications based on identity, context, policy, and app destinations using VMware Cloud Web Security. Using VMware Edge PoPs enforces security on the most optimal path between users and their applications.

Simplified operations

VMware Cloud Web Security provides a single management interface with integrated backend operations, offering customers of all sizes an easy to deploy, ready to use solution on a highly elastic cloud infrastructure.

Reduced operational cost

A cloud-based solution reduces the need for on-premises security appliances for SaaS and Internet applications. VMware Cloud Web Security offers cost savings from managing the lifecycle of physical or virtual appliances at data centers, and optionally at branch locations, when security services are distributed closer to users.

Distinct advantages of VMware Cloud Web Security

Rich user experience and higher productivity with integrated service delivery

VMware Edge PoPs ensure that security functions such as SSL decryption, security inspection and enforcement are all performed on the optimal path, and at scale, between users and their applications. This helps increase productivity by reducing latency, reducing cost by avoiding traffic backhaul to the data center, and eliminating multi-hop processing by networking and security services.

Local presence with service delivered using cloud-scale platform

VMware Cloud Web Security is delivered using the industry-proven deployment architecture powering VMware SASE™, to help customers adopt security services with ease and agility. Customers can deploy security services faster, accelerate migration from on-premises to cloud security services, stay compliant with local regulations, and gain visibility into application and employee activities. The global network of VMware Edge PoPs administers security closer to the user, on the optimal path to SaaS and Internet application destinations.

Single management pane

Seamless alignment between security policies and application policies ensures consistent security enforcement. A centralized VMware Edge Cloud Orchestrator™ offers a single pane to manage security services and network services as a converged stack. The VMware Edge Cloud Orchestrator offers administrative separation between network and security teams with support for Role Based Access Control (RBAC). This helps security teams configure security policies that the network team can assign to business policies for application

traffic. IT does not have to deal with siloed management tools to configure policies. Using a centralized policy portal, IT can administer security across the distributed enterprise without any blind spots. NetOps, SecOps, CSO, CIO and Compliance teams can get common and coherent visibility into network performance and security posture.

Use cases

Control web access

VMware Cloud Web Security ensures only authorized users have access to SaaS and Internet applications and enforces policies for safe browsing from anywhere. Websites are categorized based on risks such as known malware and phishing sites, and behavior including gambling or promoting violence. Security admins can limit exposing the attack surface, tighten security posture, and ensure compliance with the organization's Acceptable Use Policy (AUP).

Protect against attacks from document downloads and email attachments

VMware Cloud Web Security ensures users and infrastructure are protected against malware attacks from known viruses using the latest threat intelligence. The solution protects against zero-day malware with sandbox support where file behavior is inspected in a contained environment. Employees can safely download documents, access emails and open attachments without becoming a target of phishing or ransomware attacks.

Visibility and control for SaaS applications

With VMware Cloud Web Security, IT can get visibility into user activities when they access SaaS applications. The solution uses inline Cloud Access Security Broker (CASB) capabilities to help set policies for different actions users can undertake based on application type. For example, IT can determine that full-time employees can have login access, download access, or upload access for file type applications such as Box, Dropbox etc., but summer interns cannot download files. The solution also provides control and security when employees navigate between enterprise and social applications. For example, users are allowed to download a file from Dropbox, but they cannot attach any file to their LinkedIn email.

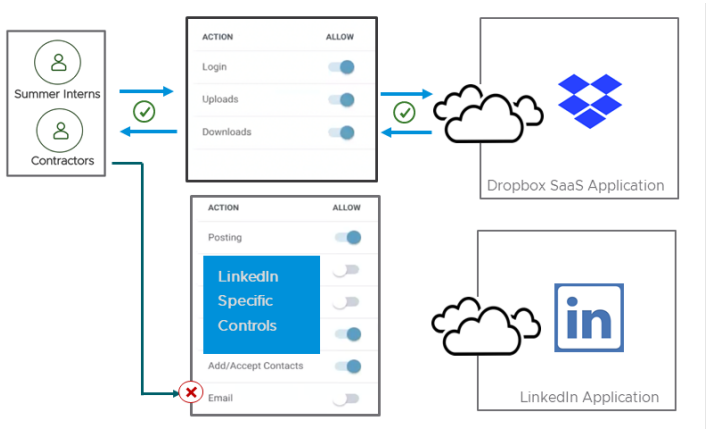

Figure 2: Granular controls for enterprise and social applications

Protect sensitive data, ensure compliance

VMware Cloud Web Security prevents sensitive data from leaving the enterprise premises. The solution monitors, detects, blocks, and reports data exposure and helps address compliance needs in many industries including healthcare, retail, finance, manufacturing, government, utilities, transportation, and hospitality, to name a few. Having a single management pane smooths operations by significantly reducing complexity and offering a common view for communication among multiple operations teams across networking, security, and compliance.

VMware Cloud Web Security features

VMware Cloud Web Security policies can be configured to inspect browser-based and non-browser web applications. For browser-based applications the solution supports application traffic on standard and non-standard web ports. Following are the list of features supported in the solution.

URL filtering

VMware Cloud Web Security limits user interaction to specific categories of websites and controls employee web browsing with granular policies via user, user groups, or IP. The solution protects users against web sites spreading malware, stealing information, or hosting inappropriate content.

Geographic region-based filtering

This capability enables IT to block or allow internet traffic based on the geographic region of the content. The solution gives a choice of over 250 countries to configure the rules.

Content filtering

The solution enables security teams to reduce the attack surface by specifying the type of content that can be uploaded or downloaded. Content filtering rules can be applied to executables, files, documents, and archives. For example, IT

could allow downloading PDFs, Word documents, Zip files and PowerPoint documents while preventing Linux and Windows executables.

Content inspection (anti-malware, anti-virus) and sandbox

VMware Cloud Web Security protects users and infrastructure from malware content in active web sites, documents, and email attachments. The solution provides safeguards from known virus and zero-day malware attacks.

Cloud Access Security Broker (CASB)

IT admins need visibility and control into sanctioned and unsanctioned applications that are in use by the enterprise. VMware Cloud Web Security offers visibility and control into SaaS and web applications that users access. The solution helps IT admins determine which applications users access and what activities they can perform with those applications. The solution provides generic controls for all applications while offering flexibility to specify controls specific to applications.

Data loss prevention (DLP)

Data loss prevention helps IT ensure sensitive data does not leave the enterprise perimeter. DLP helps enterprises adhere to compliance requirements like HIPAA, PCI, GDPR and other data privacy laws. VMware Cloud Web Security inspects content, detects exposure of sensitive data, either blocks or monitors it by policy, and provides a detailed audit trail. The solution has a rich dictionary of data identified as sensitive information and offers the flexibility to create custom definitions. It identifies data types deemed sensitive by file types, regular expressions, or set data type using the data dictionary. The audit trail includes information about the user, data exfiltrated, timestamp, destination domain, file type, file name, and action taken, among others.

Analytics and security dashboards

Security admins need visibility into each user's web browsing activity. VMware Cloud Web Security logs every session and every threat detected. Detailed information including user ID, browser used, threat discovered, threat origin, vulnerable sites and threat types help security and forensics teams to analyze and adjust security posture. Security dashboards provide coherent visibility into user activities and the threat landscape, and help admins mitigate exposure. Customers can also use APIs to pull the logs to external SIEM tools.

SSL proxy

A large percentage of web applications are SSL encrypted, creating the need to decrypt traffic and inspect content for stronger security. VMware Cloud Web Security addresses the needs arising from traffic growth, support for new applications, and introduction of new ciphers.

VMware Cloud Web Security leverages the global network of VMware Edge PoPs to offer a scalable solution that decrypts large volumes of ever-increasing web application traffic. The solution also helps enterprises bypass SSL decryption when users access personal finance or healthcare sites, or to comply

with local privacy laws. The solution offers an easy-to-use exception page in the UI to configure bypass configuration.

User and user group policy, authentication

The solution enables admins to set and manage policies for specific users, user groups and content types (all content, risky content, uncategorized content.) Admins can also create exception policies for users, user groups and content types. VMware Cloud Web Security integrates with SSO and IAM solutions with SAML support for user authentication.

SaaS tenant restriction

This capability helps customers specify the list of tenants that users on their network are permitted to access. For example, you may wish to allow access to the Office 365 corporate account for all employees but forbid them from accessing their personal accounts.

Deployment options

VMware Cloud Web Security can be deployed with one of the following options:

- **VMware SD-WAN™**: Administers security for traffic carried over a VMware SD-WAN overlay network when users located in branch, campus, office or at home access SaaS and Internet applications.
- **VMware Secure Access™**: Enterprises can deploy VMware Secure Access for their remote and mobile workforce and protect users with VMware Cloud Web Security when they access SaaS and Internet Applications.
- **VMware SD-WAN and VMware Secure Access**: Enterprises focused on employee productivity whether they are in the office or at home get the flexibility of deploying VMware Cloud Web Security with VMware SD-WAN and VMware Secure Access.
- **Web Proxy**: Enterprises that need to protect their remote users accessing web applications can direct browser traffic to VMware Cloud Web Security with a simple PAC (proxy automatic configuration) file download to the end-user devices. With this option, customers can accelerate adoption of VMware SASE by first deploying VMware Cloud Web Security, then onboarding other services such as VMware SD-WAN and VMware Secure Access in the future.
- **VMware SD-Access™**: Enterprises adopting VMware SD-Access as their remote access solution can use the Web Proxy to direct internet-bound traffic to VMware Cloud Web Security.

Licensing

Customers have flexible options to purchase VMware Cloud Web Security based on the number of users or based on site bandwidth. The solution can be purchased as a subscription offer for a 1-year, 3-year or 5-year term. Cloud Web Security can be purchased as a standalone solution with web proxy deployment. Cloud Web Security can also be purchased with VMware SD-WAN, VMware SD-Access, or VMware Secure Access. The solution can be purchased as a Standard or Advanced subscription edition.

A Standard license offers layered defense for customers interested in controlling web access, ensuring threat protection, and gaining visibility into SaaS applications.

The Advanced license includes all capabilities available with the standard edition and further tightens security posture. This edition supports advanced sandbox capabilities, helps IT admins determine what actions users can undertake with SaaS apps, and prevents sensitive data from leaving the enterprise premises.

Standard license	Advanced license
SSL inspection	All features of Standard license
URL filtering	Advanced sandbox*
Geographic region-based filtering	Cloud Access Security Broker (CASB) control
Anti-virus (malware) protection	Data Loss Prevention (DLP) visibility and control
Basic sandbox*	
Cloud Access Security Broker (CASB) visibility	
SaaS tenant restriction	
SIEM logging	

*Refer to the Basic and Advanced Sandbox table below for details.

Additional details

VMware Cloud Web Security supports SAML version 2 to connect to Identity Providers and SSL Proxy support for TLS 1.2. VMware Cloud Web Security can be purchased as a bandwidth-based license or a user-based license.

Learn more

- VMware Cloud Web Security: *sase.vmware.com/products/cloud-web-security*
- VMware SASE: *sase.vmware.com*

		Basic Sandbox	Advanced Sandbox
Document Types	Engineering Application		✓
	Productivity Apps		✓
	Word Processors		✓
	Spreadsheets		✓
	Presentation tools		✓
File Types	Scripts and Executables	✓	✓
	Archives and Compressed packages	✓	✓
	Multimedia		✓
	Calendar		✓