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 when users access SaaS applications, and ensures compliance. Cloud Web Security is delivered through a global network of VMware SASE PoPs to ensure optimal access to applications.

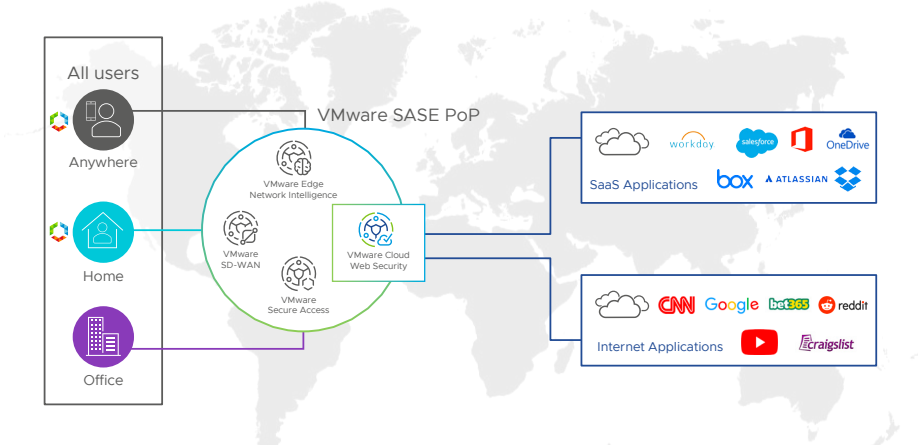

FIGURE 1: VMware Cloud Web Security protects user traffic accessing web applications

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 a global network of SASE points of presence (PoPs), it brings security closer to users while ensuring that users are nearer to 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's global network of SASE PoPs ensures that security functions such as SSL decryption, security inspection and enforcement are all performed on the optimal path between users and their applications. This helps increase productivity by reducing latency, reducing cost by avoiding traffic backhaul to the data center, and by 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 the VMware SASE Platform™, 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 SASE 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 Orchestrator offers a single pane to manage security services and network services as a converged stack. The 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 such as 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.

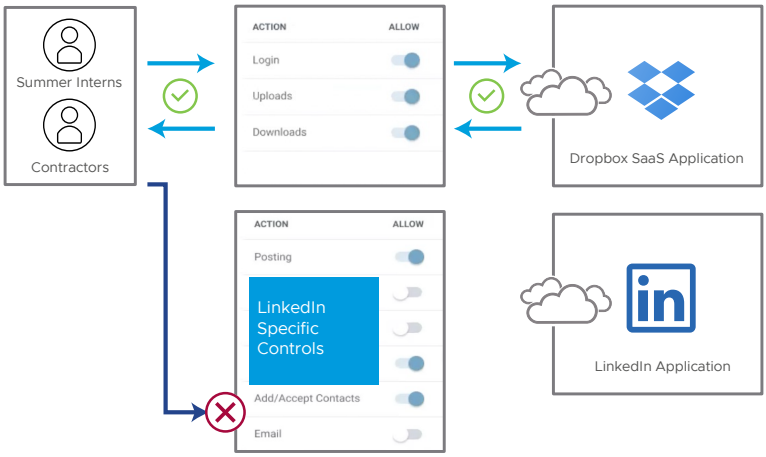

FIGURE 2: Granular controls for enterprise and social applications

Compliance, regulation and audit

Compliance needs in healthcare or retail require logging, alerting and automated responses to identify, prevent, trace, and isolate threats that impact the network, data, and resources. 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

URL filtering

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

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.

ADDITIONAL DETAILS

VMware Cloud Web Security supports SAML version 2 to connect to Identity Providers and SSL Proxy support for TLS1.2.

VMware Cloud Web Security can be purchased as a bandwidth-based license or a user-based license.

LEARN MORE

- VMware Cloud Web Security website, *sase.vmware.com/products/cloud-web-security*
- VMware SASE website, *sase.vmware.com*
- VMware SD-WAN web page, *sase.vmware.com/sd-wan*
- VMware Secure Access web page, *sase.vmware.com/products/vmware-secure-access*

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.

Web logs 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 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 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. Cloud Web Security addresses the needs arising from traffic growth, support for new applications, and introduction of new ciphers. The solution also helps enterprise bypass SSL decryption when users access personal finance or healthcare sites, or to comply with local privacy laws.

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.

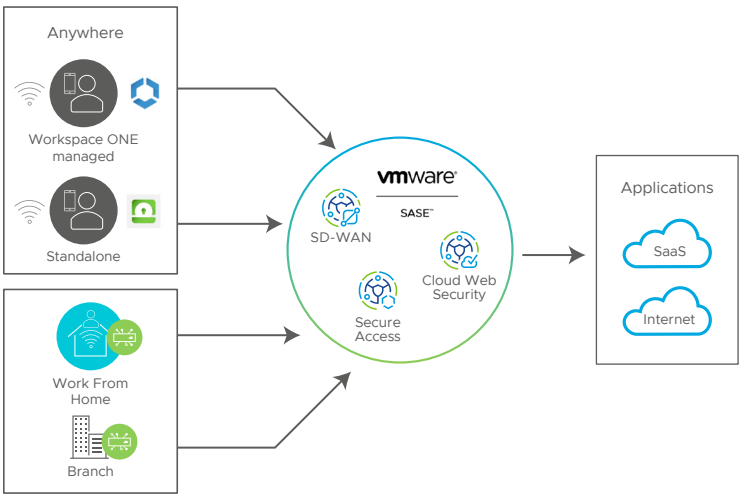

FIGURE 3: VMware Cloud Web Security protects work from home, office, and anywhere users