VMware Cloud Web Security

VMware Cloud Web Security is a cloud-hosted service that protects users and infrastructure accessing SaaS and Internet applications from threats, offering visibility, control, and compliance.

Cloud Web Security™

BENEFITS OF VMWARE CLOUD WEB SECURITY

- Rich user experience and higher productivity with integrated service delivery
- Local presence with service delivered using cloud-scale platform
- Single management pane
- Pervasive security for anywhere users

COMMON USE CASES

- Web security for safe browsing from anywhere
- Email and document download protection
- SaaS application visibility and control with per-app policies
- Ensuring compliance, with less complexity and a common management view

Enterprise adoption of SaaS and Internet applications has increased exponentially. However, IT-sanctioned applications such as Microsoft 365 make up a small percentage of the overall landscape. Many SaaS and Internet applications used by lines of business and employees are consumed without IT consent or administration.

While these apps are important for business productivity, they pose risks because there is little to no IT oversight. Risks include advanced threats, malware, and exposure of data by accident or intent. According to Verizon's 2020 Data Breach Investigations Report[1] about 43% of breaches involve web applications.

With the growth in bring-your-own-device (BYOD) plans and IoT devices, the heterogeneity and number of devices digitally connected on the network have grown astronomically, increasing the potential attack surface.

The traditional enterprise network perimeter has all but vanished. Users expect a secure and seamless experience when they access enterprise applications at any time, from any place, and on any device. In addition, employees want to navigate between enterprise and personal applications, especially on BYOD devices, without the fear of security threats or worry about compliance violations. IT teams want to ensure they can protect users and infrastructure in a way that does not impede employee productivity.

Legacy security for modern apps is a mismatch

Legacy web security solutions lack the agility to cope with the dynamic, contextual nature of applications and personalized web sites. These solutions deployed on-premises introduce unwanted latency because of suboptimal routing, increasing the cost of WAN usage and delivering a poor user experience.

A large percentage of Internet and SaaS applications are encrypted and require deeper inspection. Appliance-based solutions lack the scalability required to inspect encrypted application traffic as applications adopt newer cyphers or newer applications are consumed. Lack of visibility and control of these apps places a significant burden on IT teams tasked with assessing risk, security, privacy, compliance, and other factors to determine their safe use.

Enterprise pain points for application security include:

- **Compromised security:** There are over 16,000 known critical vulnerabilities, according to the CVE Details database[2]. Using a patchwork of security functions results in gaps and exposure to threats that are polymorphic in nature. This approach lacks coherent visibility and control, limiting the ability to tighten the security posture against a changing threat landscape and a widening surface of attack. Security services and network services deployed as isolated stacks can result in mismatch while translating security policies to network policies. This can also lead to inconsistent policy implementation depending on user location, whether at home or in a branch or in any other location, further impacting user experience.
- **Lack of agility:** With most web applications using HTTPS protocol, the demand for scale continues to grow as more and more traffic needs to be decrypted. Legacy appliance-based security runs into scale challenges and lacks the agility to respond to emerging business requirements. Deployments using virtual appliances are subject to periodic upgrades that require considerable planning and downtime.
- **Increased complexity and higher cost:** Security capabilities deployed in the data center, and optionally distributed at the edges, create management challenges for IT. This is driven in part by the complexity of managing the life cycle and refresh cycle of a large number of physical and virtual appliances. The need to design and operate a distributed reliable system of security appliances drives up the total cost of ownership. Backhauling SaaS and Internet traffic to the data center before routing it to cloud destinations increases bandwidth and adds unnecessary cost of MPLS links.
- **Poor user experience for the anywhere workforce:** Work-from-anywhere employees need seamless and secure access to all their applications without being forced to traverse the enterprise network for security enforcement at the data center. This backhauling introduces latency, which causes inconsistent user experiences based on user location—and a significant loss of productivity.

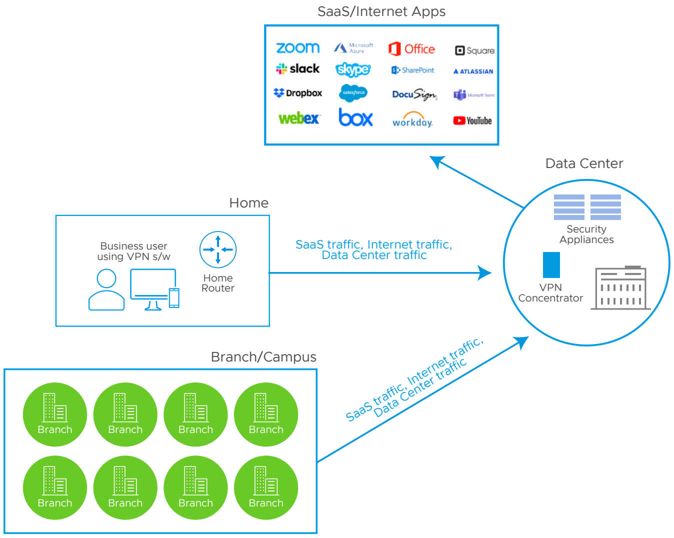


FIGURE 1: On-prem security with SaaS traffic backhaul increases cost and affects productivity

Without a better option, enterprise security teams have responded to the changing threat landscape by extending a patchwork of legacy security solutions. They are difficult to integrate and manage, leaving blind spots in the security implementation. Security personnel need a solution that protects users and infrastructure while accessing applications from any location, with visibility and control, when employees use both sanctioned and unsanctioned SaaS applications.

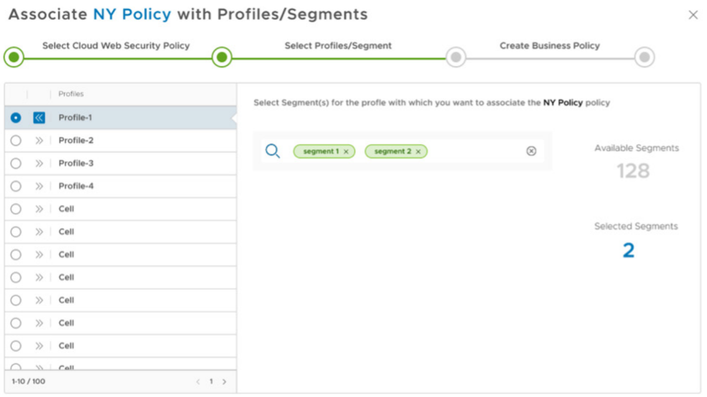
Introducing VMware Cloud Web Security

VMware Cloud Web Security is a cloud-hosted service that protects users and infrastructure accessing SaaS and Internet applications from a changing threat landscape, offers visibility and control, and ensures compliance. Part of VMware SASE (secure access service edge), Cloud Web Security is delivered through a global network of VMware SASE points of presence (PoPs) to ensure optimal access to applications.

Cloud Web Security extends the advantages of the efficient and reliable service offered by VMware SD-WAN and VMware Secure Access to connect users located anywhere to SaaS and Internet applications, with security enforcement applied along the optimal path.

Cloud Web Security delivers the following distinct benefits:

- **Rich user experience and higher productivity with integrated service delivery:** The global network of VMware SASE PoPs ensures that security functions like SSL decryption, security inspection, and enforcement are all performed on the optimal path between users and their applications. Eliminating multi-hop processing of networking and security services reduces latency, bandwidth consumption, and cost, and ultimately helps increase productivity.
- **Local presence with service delivered using cloud-scale platform:** 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 and remove barriers in migrating from on-prem to cloud security services, stay compliant with local regulations, and gain visibility into application and employee activities.
- **Single management pane:** A centralized orchestrator offers a single pane to manage security services and network services as a converged stack. IT does not have to deal with siloed management tools to configure policies. Seamless alignment between security policies and application policies ensures consistent security enforcement. 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.



Associate NY Policy with Profiles/Segments

Profiles

● Profile-1
○ Profile-2
○ Profile-3
○ Profile-4
○ Cell
○ Cell
○ Cell
○ Cell
○ Cell
○ Cell
○ Cell
○ Cell

1-10 / 100 ‹ 1 ›

Select Segment(s) for the profle with which you want to associate the **NY Policy** policy

segment 1 × segment 2 ×

Available Segments 128

Selected Segments 2

FIGURE 2: Orchestrator UI workflow to attach security policy to SD-WAN network segments

- **Pervasive security for anywhere users:** VMware Cloud Web Security offers comprehensive security coverage for the entire spectrum of users ranging from power users to light users working from anywhere. Because security policy follows the user, Cloud Web Security applies consistent policies no matter where users are located, delivering a seamless experience for the distributed anywhere workforce.

Solving for agility, user experience and more

Cloud Web Security can help address the issues that enterprise IT teams see daily, including:

- **Agile security posture:** Cloud Web Security enables enterprise security teams to adapt to the changing threat landscape and business needs without leaving gaps in the security posture. The cloud-hosted solution scales with processing needs to support new cyphers, new applications, and traffic growth, to adapt to changing business environments. The cloud-based solution analyzes and offers actionable insights to tighten the security posture.
- **Seamless and secure access for the anywhere workforce:** Cloud Web Security applies consistent policies based on identity, context, policy, and app destination whether the users are on-site or at home. This eliminates the need to manage multiple policy sets depending on the user location. Using a global network of SASE PoPs the solution brings security closer to the users while ensuring that users are nearer to their applications.
- **Simplified operations:** Cloud Web Security provides a single management pane to configure security and networking policies. Using the VMware SD-WAN Orchestrator, IT can ensure security policies are deployed across the network to offer a consistent experience without any mismatch in policy implementation. Network and security teams get a common view of network state and security posture to focus on addressing business needs rather than spending time interpreting data from multiple management solutions.
- **Reduced operational cost:** Cloud Web Security reduces the need for on-prem security appliances for SaaS and Internet applications. The solution offers cost savings from managing the life cycle and refresh of physical or virtual appliances at the data centers, and optionally at branch locations when security services get distributed closer to the users. The majority of web applications are SSL encrypted and require deeper inspection to determine the threat. The solution scales easily when it identifies web content, decrypts and analyzes traffic, enforces policies and encrypts traffic. Additional cost savings also come from reducing bandwidth consumption on MPLS links without the traffic backhaul to the data center.

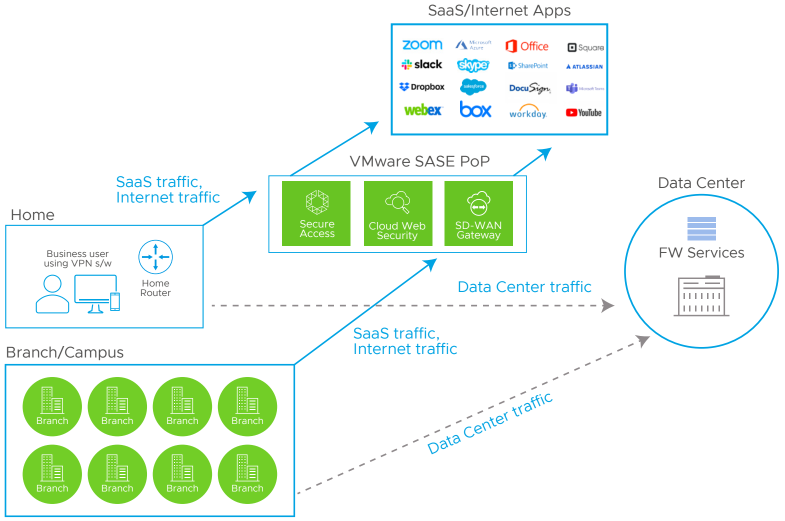


FIGURE 3: Security administered on the optimal path between users and SaaS/ Internet applications

Use cases

Cloud Web Security addresses the following use cases:

- **Web security:** Cloud Web Security acts as a central security control point to ensure only authorized users have access to SaaS and Internet applications, and it enforces policies for safe browsing from anywhere. Security admins can configure web access policies based on risk, behavior, locations, user groups and more. The solution analyzes risks to determine which URLs, applications, or users are vulnerable to bring in malware, detect if there is any polymorphic malware, looks for indicators of compromise, and determines the action to be taken to limit exposure. The solution also protects infrastructure from infected devices.
- **Email and document download protection:** Phishing is a common tactic used to trick users to click on a malicious link or download a malicious document sent by a seemingly trusted source. Cloud Web Security ensures that employees can safely download email attachments without becoming a target of phishing or ransomware attacks. According to Verizon's 2020 Data Breach Investigations Report, 46% of organizations received malware via email1. With Cloud Web Security, email attachments and documents are inspected to determine whether downloaded content is benign or infected. The solution ensures users and infrastructure are protected from known and Day 0 malware attacks with a combination of file hash checks, anti-virus protection, and sandboxing for unknown signatures.
- **SaaS application visibility and control:** Cloud Web Security helps IT 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, while restricting summer interns from file downloads. 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.

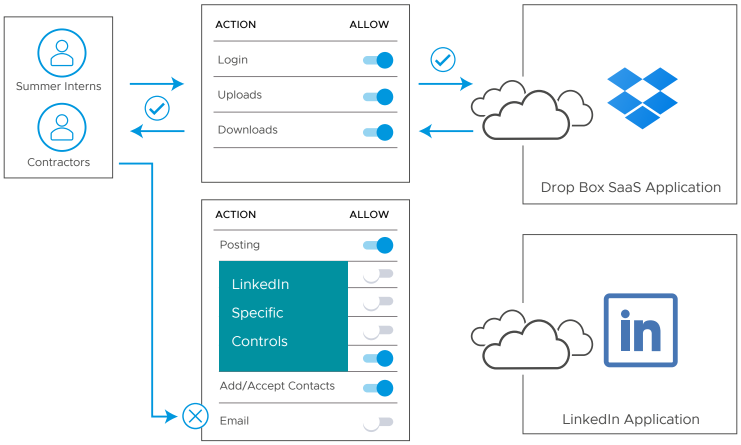


FIGURE 4: Granular controls for enterprise and social applications

- **Ensuring compliance:** 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 helps operations significantly reduces complexity and offers a common view for communication between multiple operations teams across networking, security, and compliance.

Cloud Web Security is offered through the global network of VMware SASE PoPs and can be delivered together with VMware SD-WAN or VMware Secure Access.

Footnotes:

1. Verizon Data Breach Investigations Report: *https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf*
2. Common Vulnerability and Exposure Details: *https://www.cvedetails.com*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com