Gain Control of Your SaaS Apps

VMware Cloud Web Security with CASB

- How do you protect something that you cannot see? A key capability of VMware Cloud Web Security and the VMware SASE portfolio, cloud access security broker (CASB) provides IT teams with complete visibility into all SaaS applications used by the enterprise and control over users' actions on these applications.
- Cybersecurity challenges arising from shadow IT can now be addressed without impairing business productivity.

Software-as-a-service (SaaS) adoption has accelerated across enterprises of many sizes and sectors. While the migration to cloud and the extensive usage of SaaS has proven benefits including reduced costs, greater productivity, and increased flexibility, it has significantly widened the threat landscape and attack surface that organizations are now exposed to.

The fast adoption of SaaS applications has caused a major shift in the IT delivery model from a traditional centralized one to a more efficient, decentralized one. In the traditional model, any department that wanted to onboard a new web application would involve corporate IT and follow a robust process that typically included:

- Completing due diligence of the SaaS provider's reputation and security controls
- Performing technical security assessments using industry standards such as Open Web Application Security Project (OWASP)
- Installing and maintaining the software

With a centralized model, visibility and control were straightforward. However, that model is not congruent with the migration to cloud and SaaS, which can provide lower overall costs and improved productivity.

In the new de-centralized model, organizations achieve higher productivity and speed-to-market given how easy SaaS applications are to onboard and use. However, allowing business users to subscribe to new unsanctioned SaaS applications without the knowledge and oversight of corporate IT has contributed to the "shadow IT" phenomenon, exposing the enterprise to significant cybersecurity challenges.

Easy access to apps creates blind spots

Using unreliable software/service

Users of unsanctioned applications do not have the bandwidth or technical expertise to conduct adequate due diligence on the SaaS vendor with the same

Key benefits

- CASB is an effective approach to mitigating cybersecurity risks caused by shadow IT
- The VMware CASB solution provides real-time visibility and control across an enterprise's SaaS portfolio
- CASB reduces IT and security personnel's workload and simplifies policy enforcement

Learn more

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

rigor that IT and security teams do. This could lead to a potential entry point for a cyberattack.

Sharing confidential information outside the organization

A user may intentionally or unintentionally share or store sensitive information outside the enterprise's network protection. Without adequate data protection controls (e.g., data loss prevention, encryption), the sensitive information can leak out, resulting in financial and reputational damage to the firm.

CASB provides visibility into SaaS apps

A common industry approach to tackle unsanctioned application usage is cloud access security broker (CASB). CASB provides visibility into SaaS applications used by the enterprise and enables granular control by IT.

A CASB secures traffic between an enterprise and cloud providers. Located either on-premises or in the cloud, it monitors communication between users and cloud services, enforcing policies and securing traffic. CASBs provide a standardized user experience while enhancing control over session visibility and traffic management.

VMware's approach to CASB

VMware Cloud Web Security™, part of VMware SASE™, offers a cloud-hosted CASB solution that applies policies inline on traffic going between end users and SaaS applications. This helps IT take any action necessary before the traffic reaches its destination. Through VMware's CASB solution, organizations can gain enhanced governance over the discovery and usage of SaaS applications through:

- **Application discovery and visibility**: The first step in a security strategy is to determine what you are trying to protect. CASB offers a complete view of all SaaS applications in use along with their associated risk scores. IT teams can monitor the risk level against the organization's risk tolerance, for better governance and auditability.

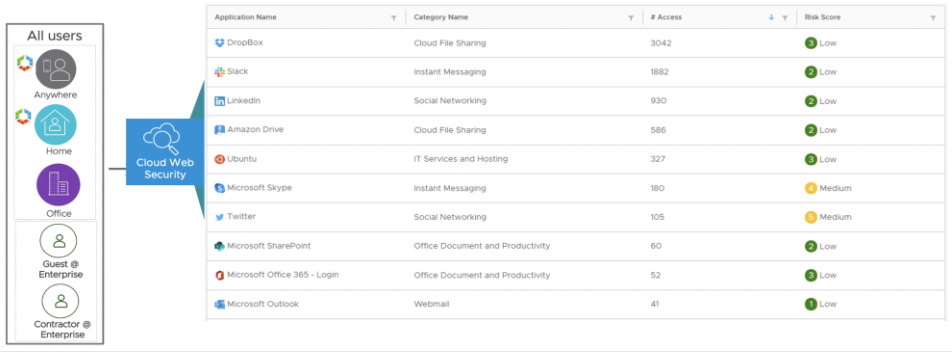

Figure 1: CASB dashboard shows SaaS applications in use and their risk scores

- **Activity control through fine-grained policies**: IT administrators can easily and consistently set fine-grained security policies to control the interactions that specific users and user groups can have with a particular application. For example, for a low-risk application, users would be permitted to log in, upload and download files. For a high-risk app, users would be allowed only to upload files.
- **Security Information & Event Management (SIEM) integrations**: Apart from providing complete visibility into user activities on the VMware SASE Orchestrator dashboards, VMware Cloud Web Security has API support to integrate with commonly used SIEM and log analytics tools.

Why choose VMware Cloud Web Security for your CASB requirements?

An effective cybersecurity solution needs to offer benefits that extend beyond just the technology to include people and processes. In addition to providing clear technological benefits, VMware Cloud Web Security automates several routine tasks that IT stakeholders must undertake. The solution helps reduce operational burden and offers these benefits for people and processes:

Beneficiary	Stakeholder(s)	How does CASB help?
People	Senior management	• Accelerates strategic priorities • Enhances oversight and governance • Promotes effective risk management
	IT & security teams	• Increases visibility and control over SaaS portfolio • Helps meet regulatory and compliance requirements • Simplifies policy creation

Beneficiary	Domain(s)	What does VMware Cloud Web Security provide?
Process	Asset management	• Complete visibility into SaaS portfolio • Inputs for business impact
	Cybersecurity risk management	• Risk management of SaaS portfolio • Convenient risk tracking and monitoring
	Compliance	• Security baseline standards • Compliance with regulatory requirements and security baselines
	Security operations	• Single pane of management • Simplified policy management across user groups and applications
	Security log management	• API integrations with major logging tools

VMware Cloud Web Security, offered as a part of the VMware SASE solution, delivers security with operational simplicity and a rich user experience.

Item No: SDWAN-1023-Control-SaaS-Apps-CWS-CASB-so-0822