



Making SaaS Safe

7 Requirements for Securing Cloud Applications and Data

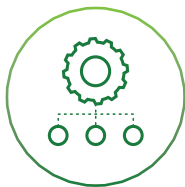


Introduction: The Reality of SaaS in the Enterprise

ADVANTAGES



**Ease of use
and cost-
effectiveness**



**Rapid
deployment**



**Anywhere,
anytime access**



**Automatic
upgrades and
maintenance**

CHALLENGES



**Protecting
against data loss
and leakage**



**Threats to
data privacy**



**Breaches of
confidentiality**

As SaaS-first strategies become more commonplace, IT and security leaders must address the unique challenges of securing software-as-a-service (SaaS) usage and corporate data stored within cloud applications. The existing on-premises security stack protecting the enterprise is no longer sufficient when users take business-critical and/or sensitive data with them into the cloud.

When using SaaS applications without the knowledge or approval of IT—practicing so-called “shadow IT”—employees often do so without the benefit of security and governance best practices, controls, and oversight. That could leave sensitive data at risk of inadvertent public exposure or theft by cybercriminals and expose the enterprise to numerous other security risks.

The reality is that even when SaaS applications are vetted and sanctioned by the IT department, security gaps can remain, leading to data leaks, regulatory noncompliance, malware propagation, and more.

Read on to learn about seven requirements for SaaS security and how they can help you protect your employees, data, and company from cyberthreats when using SaaS applications.

1

Discover Employee Use of Unvetted SaaS Applications



Scenario

One of your company's managers subscribes to a new SaaS-based project management tool for the team working on a confidential new product line. The manager begins storing sensitive data that includes intellectual property in the application.



Why You Should Care

Employees can try out and self-provision SaaS applications in mere minutes without needing to contact IT or request approval from the procurement department. This gives users unprecedented control of software selection, administration, and usage—often without the IT department's approval or oversight.



Security Implication

Use of unvetted SaaS applications can introduce significant blind spots for your security team, including data loss and leakage, misconfigured or missing security controls, and noncompliance with privacy and industry regulations.



Best Practice

As SaaS adoption expands exponentially, manual discovery of SaaS usage in the enterprise becomes rapidly untenable. Instead, to quickly identify risk—and extend appropriate security controls—your organization needs an automated way to continuously discover all SaaS applications in use by employees.

1 Discover Employee Use of Unvetted SaaS Applications: Important Questions



How much visibility does your team have into the use of unsanctioned SaaS applications?



Are you relying on manual review of log data to uncover usage of unsanctioned SaaS applications?



Is sensitive data stored in unsanctioned SaaS applications, and if so, do the applications have appropriate security controls?

What's a CASB, and How Can It Help?

Coined by Gartner, the term “cloud access security broker” (CASB) refers to technology that delivers granular visibility and precise control over the enterprise usage of cloud applications as well as governance and protection for cloud-based data. Unlike other security tools your enterprise may use, CASBs offer cloud-specific capabilities that address security gaps in your organization's use of cloud services, including identifying shadow IT risk through visibility into application usage across your network.

2 Protect Sensitive Data in SaaS Applications



Scenario

An employee inadvertently stores sensitive data in a publicly shared folder while using a sanctioned SaaS application.



Why You Should Care

Without proper controls, SaaS users can leak sensitive or confidential information accidentally or maliciously. One simple mistake, such as a mis-typed email address, can lead to data ending up in the wrong hands.



Security Implication

Many organizations aren't aware that security is a shared responsibility with the cloud service or application provider. Although the cloud service provider secures the components of the cloud infrastructure, it's the SaaS customer's responsibility to protect users and data.



Best Practice

Implement advanced data loss prevention (DLP) capabilities using an API-based approach to scan for sensitive information stored within SaaS applications. Compared to in-line, an API-based approach provides deeper context and allows for automatic remediation of data-risk violations.

2

Protect Sensitive Data in SaaS Applications: Important Questions



Have you educated your IT and security teams on the Shared Responsibility Model for security in the cloud?



Do you have insight into which SaaS applications have sensitive or company confidential data stored in them?



Can you control the types of data that employees are uploading, storing, and sharing in the cloud?

How the Right CASB Can Help

Choose an offering that can scan and classify all data stored within SaaS applications. Some CASB vendors take advantage of supervised machine learning algorithms to categorize data and identify files containing sensitive information. Once the information is discovered, the CASB should check the information assets for any incidents or exposures as well as compliance with regulations or corporate policies.



3 Secure Your Weakest Link—SaaS Users



Scenario

A cybercriminal uses a phishing email to steal the credentials of an employee with administrative access to a SaaS application where sensitive data is stored.



Why You Should Care

Cybercriminals focus on compromising user credentials because it's often easier than trying other attack methods to get access to your cloud applications and data. With the right credentials in hand, an attacker can use them to exfiltrate data for malicious purposes or sale on the black market.



Security Implication

Just as it's your responsibility to protect your data in SaaS applications, you also need to protect your company's users. Managing access rights to numerous SaaS applications is complex, leading to mistakes such as employees being given higher access rights than they need.



Best Practice

Start with user training and interactive coaching to identify and help change risky behavior. Then, give your security team tools to help them monitor and govern SaaS application permissions. Look for a product with robust access controls, including:

- Multi-factor authentication (MFA) to strengthen access control
- Role-based access control
- Protection for administrative accounts
- User access monitoring that can detect malicious or risky behavior

3

Secure Your Weakest Link—SaaS Users: Important Questions



Are you following least-privileged access best practices, whereby users only have access to the functionality and data required for their roles?



Do you require strong authentication for privileged activities?



Can you monitor user activity and alert on suspicious behavior?

How the Right CASB Can Help

Look for a CASB with simple-to-manage policies that let you control access to SaaS applications at a granular level, defining which applications are allowed as well as the acceptable behaviors permitted within each one. With the right CASB, you can create security policies that establish access and usage controls at the network, device, and user levels. Finally, the CASB should alert you when there are anomalous activities that could indicate stolen credentials or malicious intent.

4 Enforce Compliance Requirements in the Cloud



Scenario

A member of your human resources staff uploads employee data to a shared folder within a sanctioned SaaS application. The data happens to include the health plan account number for each employee.



Why You Should Care

Personal health information (PHI), including health insurance account numbers, is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Inappropriate storage or sharing of this type of content could mean your company is noncompliant with the regulation and subject to fines.



Security Implication

To maintain compliance with regulations, enterprises must know where compliance-related data is being used, stored, and potentially shared. Without deep visibility into SaaS usage, your security and governance teams can't enforce or prove compliance with mandatory regulations.



Best Practice

Create and enforce a consistent, granular security policy for compliance that covers all SaaS applications used by your enterprise. This includes automating compliance and reporting for all relevant regulatory requirements across your SaaS applications. Ideally, you should have the compliance report ready at the push of a button when auditors request it.

4 Enforce Compliance Requirements in the Cloud: Important Questions



Do your sanctioned SaaS applications have the appropriate, relevant, or required security certifications for compliance?



How do you currently protect compliance-related content in the cloud?



Do you know whether users are uploading data that includes personally identifiable information (PII), payment card numbers, PHI, or other sensitive information to SaaS applications?

How the Right CASB Can Help

Using advanced DLP capabilities, the right CASB lets you set and enforce granular policies to identify, monitor, and automatically protect regulated data. Look for a CASB that offers preconfigured policy and reporting templates to help you maintain compliance with common industry standards and regulations.

5 Reduce the Risk from Unmanaged Devices



Scenario

An employee downloads data from a sanctioned SaaS application onto a personal, unmanaged device. The data is then stolen and sold to a competitor.



Why You Should Care

Unmanaged devices create blind spots and increase security risks, including everything from the introduction of malware to data leakage.



Security Implication

Many SaaS applications don't have granular security controls that can recognize managed (corporate-owned) versus unmanaged devices and enforce access rules accordingly. Although some recognize and block unmanaged devices, they don't have the ability to selectively allow access to certain functionality. Completely blocking users from using their personal devices to access the SaaS applications and data they need to do their jobs effectively is not a viable option.



Best Practice

Deploy a security product that differentiates access between managed and unmanaged devices to protect against the increased security risks inherent with personal devices. For instance, you could allow downloads to managed devices but block them for unmanaged ones while enabling access to core functionality.

5 Reduce the Risk from Unmanaged Devices: Important Questions



Do you enforce MFA for logins from unknown or unmanaged devices?



Have you created separate access policies for managed and unmanaged devices?



Do you have full visibility and precise control of the content that users are uploading to and downloading from unmanaged devices?

How the Right CASB Can Help

When deployed using an in-line approach, some CASBs offer both a forward proxy (forwarding cloud traffic to a security appliance or service) and a reverse proxy (rerouting traffic to an in-line security appliance or service) mode. With reverse proxy capabilities, you can use single sign-on to seamlessly reroute users on unmanaged devices to the in-line security gateway to enforce policies. This functionality lets you secure access from any unmanaged or personal device that uses an internet browser to access SaaS applications.

6 Control Data Sharing from SaaS Applications



Scenario

One of your sales managers stores customer information, some of which is confidential, in a SaaS application. To collaborate with a third-party company on sales efforts, he shares the data by sending the third party a link to the file containing the customer data.



Why You Should Care

Because many SaaS applications make it easy for users to collaborate and share, they become highly susceptible to employees oversharing or inadvertently sharing sensitive content. The recipients of shared data may reshare the sensitive content, which further increases the risk of data loss.



Security Implication

Without deep visibility and granular control over data-sharing activities in SaaS applications, the risks of inadvertent or malicious data leakage grow as users share sensitive data, sometimes to untrusted users or applications.



Best Practice

Use an in-line approach to gain visibility into sensitive data flowing into high-risk, unsanctioned applications. Create and enforce DLP policies that control data-sharing activities in the SaaS applications employees use.

6 Control Data Sharing from SaaS Applications: Important Questions



Can you track data-sharing activity within and between the SaaS applications employees use?



Can you block or limit external data sharing based on the user, group or department, role, data type, application, or other characteristics?



What actions are taken when a violation of your company data-sharing policy is detected?

How the Right CASB Can Help

A robust CASB with integrated DLP capabilities can enforce granular, context-aware policies based on keywords, file characteristics, and other content patterns. The CASB can also quarantine users and data should violations occur. Complementing an in-line approach, a CASB using API mode can inspect existing data stored in the cloud as well as remediate existing DLP violations and threats.

7 Stop SaaS-Borne Malware Threats



Scenario

A file containing malware is uploaded to a shared folder on one of your enterprise's sanctioned SaaS applications. The SaaS application then automatically syncs across devices and users, which deploys the malicious payload to everyone using the application in your enterprise.



Why You Should Care

SaaS applications are particularly vulnerable to malware threats, making them effective distribution media for cybercriminals. Features such as automatic syncing make it easy to instantly distribute malware.



Security Implication

SaaS applications are often the first insertion points for malware and the last exfiltration points for data loss, and as such, they need to be protected from malware threats.



Best Practice

Implement threat prevention technology that works with your SaaS security to block malware and stop threats from spreading through SaaS applications, eliminating a new insertion point for malware.

7

Stop SaaS-Borne Malware Threats: Important Questions



Can you detect zero-day threats or unknown malware originating from SaaS applications?



Do you have malware analysis capabilities in place for content in SaaS applications?










Can you quarantine suspicious content or infected devices?

How the Right CASB Can Help

To prevent an insertion point and the further spread of malware across your organization, choose a CASB with integrated malware prevention capabilities. These capabilities should block known malware as well as identify and block unknown malware in content stored in SaaS applications.

Your SaaS Security Checklist

As your company evaluates CASB offerings for securing SaaS applications and data, use the seven requirements presented in this e-book to guide your assessment and define your criteria. Look for an offering that gives your security team the ability to:

-  **Discover employee use of unvetted SaaS applications**
-  **Protect sensitive data in SaaS applications**
-  **Secure your weakest link—SaaS users**
-  **Enforce compliance requirements in the cloud**
-  **Reduce the risk from unmanaged devices**
-  **Control data sharing from SaaS applications**
-  **Stop SaaS-borne malware threats**

Next Steps

Most enterprises will agree that the benefits of SaaS applications—improved agility, faster time to market, greater productivity, easier collaboration, and more—outweigh the challenges of managing their usage for proper security and governance. However, with employees using more SaaS applications every day and storing company information, including sensitive data, in the cloud, IT and security leaders must take immediate steps to protect their enterprises from data loss, malware threats, non-compliance, and other serious risks to the business. A CASB that addresses the seven requirements introduced here is the best way to bridge the SaaS security gap and protect the business while enabling it to enjoy the benefits of SaaS applications.

About Prisma™ by Palo Alto Networks

Governed access, plus pervasive protection for data, applications, hosts, containers, and serverless—this is the proper foundation for the journey to the cloud. With a comprehensive cloud security suite, Prisma helps our customers secure every step of their journey.

Prisma provides unprecedented visibility into assets and risks, consistently securing access, data, applications, and modern workloads, regardless of location. The suite helps customers deploy and adapt quickly with speed and agility as well as control operational costs and reduce complexity with a radically simple architecture.

Prisma is the most complete cloud security suite for today and tomorrow.

Learn how **Prisma** can help provide data protection, governance, and compliance to safely enable organizations to adopt SaaS.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. Making-SaaS-Safe-ebook-111819

