CASB vs SMP:

A complementary approach needed to combat Shadow IT and effectively govern the SaaS ecosystem

Managing the SaaS ecosystem has become a strategic challenge for large organisations, driven by the urgency of digitalisation, the rapid growth of SaaS applications (+18% in 2023), and the increasing autonomy of business departments in their technology choices. These trends create new opportunities and numerous challenges and risks for IT departments.

To effectively handle SaaS applications and address Shadow IT (applications used by employees without the knowledge of the IT teams), enterprises are implementing tools to help secure and govern their IT ecosystem.

> According to Gartner (Market Guide for SMP, 2022), "there are several technologies to consider when looking to get started with SaaS discovery". For example, CASB "can discover, protect, and restrict access [to these applications] based on assessed risk, conditional access policies or defined business rules, but lacks functionality to manage, automate, optimize or enable SaaS."

Organisations often face a dilemma: **is using a CASB effective enough to detect Shadow IT and effectively govern a growing Cloud ecosystem, particularly with the widespread adoption of SaaS applications? Is the implementation of another tool necessary?**

CASB: a partial answer to Shadow IT

To deal with the growing cyber threats, large organisations are increasingly deploying a Cloud Access Security Broker (CASB) to strengthen the security of their Cloud environment. It directs the connectivity of all applications through a proxy server or APIs for extensive control and monitoring of Cloud applications. This tool, acting as a guardrail, is also used by IT teams to detect Shadow IT.

CASBs offer many benefits, including:

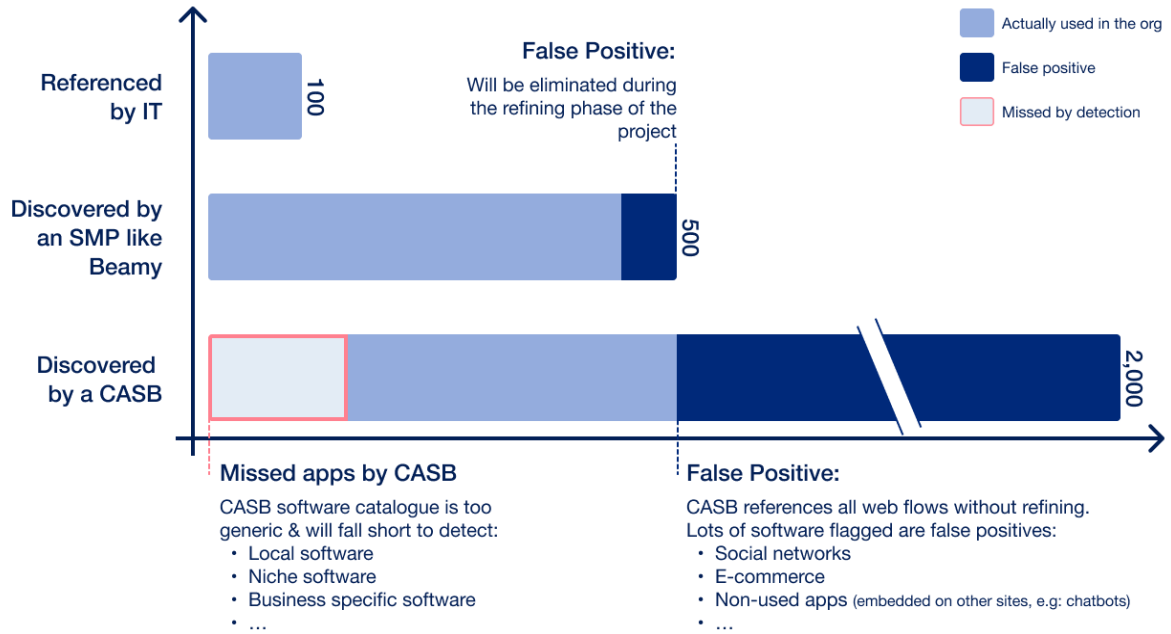
- Improving visibility into Cloud applications usage, such as users and data volume
- Enhancing monitoring of Cloud solutions to detect risky behaviours
- Discovering of Shadow IT
- Blocking access to unapproved Cloud services
- Streamlining the management of Cloud applications' configuration settings
- Enhancing control over the flow of sensitive data

This approach gives organisations visibility, control, and compliance, strengthening their protection against cyberattacks and data breaches.

Despite their crucial role in identifying Shadow Cloud (unauthorised use of Cloud services), CASBs struggle to accurately detect SaaS applications, given the rapid spread of these solutions. Representing a significant portion of Shadow IT, SaaS apps are a major challenge for IT teams. Overwhelmed by the volume and complexity of all the data collected by CASBs —often polluted with applications used for personal purposes (such as Amazon and Facebook...)—IT staff have difficulties filtering out the noise.

> **Gartner** (Market Guide for SMPs, 2022) **points out the limitations of CASBs for "managing, automating and optimizing SaaS applications".**

Discovering feature: CASB vs SMP



The Limits of CASB tools

1. **Inaccurate and noisy data:** CASBs use company logs to identify Cloud applications. However, only 1 to 2% of these logs actually relate to SaaS apps used for business purposes. This situation creates complexity in the analysis, introducing “noise” into the data and false positives (application detected but not used), requiring additional manual intervention (about 1 to 2 FTE for 1 year to process the data received)

2. **Incomplete database:** CASB databases, generally standardised, only partially reference the SaaS applications available on the market. This can lead to incomplete analysis, where some URLs detected are not correctly categorised, resulting in false negatives (around 50% of SaaS used are missed by CASB’s analysis)

3. **Limited visibility of usage:** CASBs only collect data relating to security. They do not distinguish usage, user behaviours, etc. For example, they do not differentiate between personal and professional use, increasing the number of applications identified as Shadow IT.

4. **Blind spot in detection:** CASBs do not detect duplicates, redundant applications, unused or underused, which are common cases in companies with more than 1000 employees. This failure can compromise the effectiveness of the analysis and the IS rationalisation efforts of procurement teams or IT architects.

5. **Lack of insight into usage:** CASB analysis does not capture traffic from unmanaged devices or devices outside the corporate network leading to a lack of insight into SaaS usage.

6. **Poor collaboration:** CASB is proving to be a very good tool for CISOs to maintain the security of the Cloud ecosystem. However, blocking an application is a decision that requires involving other departments (finance, security, legal, etc.). CASB is very limited when collaborating with multiple stakeholders, making the governance of SaaS ineffective in the long term.

7. **Technical complexity:** CASB architecture involves proxy, agent and API-based approaches, which can be complex, costly to deploy and require considerable time and effort to implement.

These limitations are compounded by a fundamental problem: the lack of actionable data. CASBs’ analysis capabilities tend to suffer from a deficit of actionable insight. They generally lack personalised dashboards or an in-depth understanding of usage trends, which are crucial for proactively anticipating and dealing with cyber threats.
Although some CASBs offer automated workflows for threat management, these processes are limited in customisation and complexity, which can hamper companies’ ability to respond to security incidents in an agile and effective manner.

CASB vs SMP

Criteria	Cloud Access Security Broker (CASB)	SaaS Management Platform (SMP)
Objective	Security of access and data in the cloud	Govern the SaaS ecosystem: manage, monitor, and govern the usage of SaaS apps continuously
Target / Users	CISO, IT Security teams	CIOs, IT leaders, governance teams (security, finance, legal, etc.) and business managers
Shadow IT Discovery	Shadow Cloud - often imprecise and noisy global detection including professional and personal uses	Shadow SaaS: accurate detection based on professional uses (differentiation with personal uses
Detection Source	Primarily based on logs	Mainly detection with a Web extension
App Monitoring	Very little or no information on the usage of SaaS applications	Precise information on the usage of SaaS (time spent, number of users, stickiness...) allowing for an in-depth understanding of usage patterns
Security & Compliance	Monitoring of risky behaviors, blocking unapproved access	Real-time security alerts, helps with regulatory compliance
Gouvernance	Little or no governance approach	Facilitates SaaS governance policies establishment through integrated and customised workflows
Collaboration	Limited, oriented towards security teams	Promotes cross-team collaboration through a unique platform and defined workflows
Deployment & cost	Can be complex and costly and requires significant IT resources	Often simpler to deploy and less expensive

SMP: the effective solution for governing SaaS

CASBs have developed rapidly alongside SaaS management platforms (SMPs). Although the detection of Shadow IT is a common functionality shared by both tools, CASBs and SMPs adopt a distinct approaches in regard to discovering and managing Shadow IT. CASBs focus primarily on securing Cloud applications and detecting “Shadow Cloud”. SMPs such as Beamy, on the other hand, prioritise an approach based on the governance of SaaS applications, highlighting a comprehensive understanding and ongoing monitoring of SaaS usage.

They show distinct observability focus using different input data sources and knowledge bases. CASBs delve into more specific security data like incidents, non-compliance with security policies, and the security of application services.

SMPs concentrate on a more detailed and specific investigation of SaaS applications and uncover “Shadow SaaS”. These platforms examine data such as session duration, usage level (low/medium/high), login frequency, the differentiation between

professional and personal login, and engagement duration. This emphasis on SaaS apps allows IT teams to better understand the specific uses and needs of business departments. It facilitates closer collaboration between IT teams, end-users, and other SaaS governance stakeholders (security, legal, finance, etc.).

> According to Gartner (Market Guide for SMPs, 2022), **"SMPs provide centralized tools to identify, manage, automate, optimize, govern, and enable SaaS used by employees while enhancing the protection of identities and data."** Gartner (Market Guide for SMP, 2021) **also predicts that "by 2026, 50% of organizations using multiple SaaS applications will centralize management and usage metrics of these apps using an SMP tool".**

The benefits of an SMP

- **Comprehensive detection:** SMPs offer a central platform cataloguing all SaaS applications used, including those in Shadow IT. Continuous detection, especially through a web extension, ensures complete and real-time visibility of the SaaS ecosystem. A key component for effective governance. To learn more about ongoing detection, click here »
- **Monitoring & optimisation:** Thanks to real-time monitoring, particularly via the web extension, SMPs deliver a deep understanding of SaaS usage. With a wide range of usage data (time spent on an application, number of users, retention on the application, and more), IT teams can quickly identify duplications, underused apps, and usage trends. This enables proactive observability of their ecosystem, mitigating potential risks and facilitating targeted adaptation of management, optimisation, and governance strategies.
- **Security and compliance:** By providing precise data on SaaS usage and applications' criticality level, SMPs help identify the most sensitive and urgent applications requiring attention. This enables security and compliance actions to be prioritised. Sending real-time alerts (use of prohibited applications, usage spike, significant usage drop and more) enables quick actions to tackle risks and ensure a safe and efficient SaaS environment.
- **Governance & collaboration:** Some SMP tools encourage collaborative governance by involving every stakeholder (IT, finance, legal, business, etc.). IT teams can establish robust governance frameworks thanks to automated and customisable workflows. Business departments then become autonomous in selecting and deploying their preferred apps while contributing to their management within a defined and secure framework. This fosters the adoption of best practices and guarantees informed decision-making aligned with the company's strategic objectives. Productivity and operational efficiency are improved, simplifying technology management and collaboration between departments.

CASB & SMP: complementary approaches

Next-generation SaaS Management platforms, such as Beamy, include a number of essential features for effective management and governance of the SaaS ecosystem.

However, they do not substitute the advanced security capabilities offered by CASBs. Therefore, rather than opting for one over the other, large enterprises would benefit from adopting a combined approach, leveraging the complementarity of these two tools.

> **Gartner** (Market Guide for SMPs, 2021) **states that "Rather than competing offerings, tools like CASBs will work in conjunction with SMPs."**

SaaS Management Platforms operate in synergy with existing company tools, such as ServiceNow, Zcaler, Broadcom, etc. See the Gartner diagram.

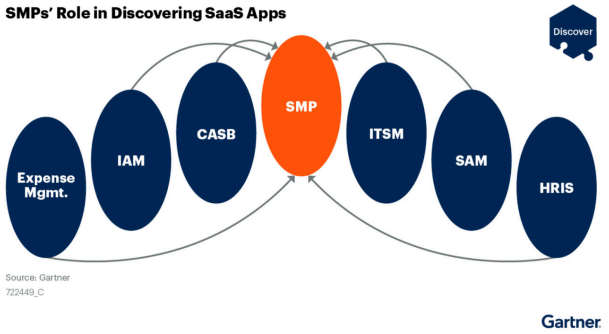
Gartner Markets Adjacent to SMP

Integrations between a CASB and an SMP can be highly beneficial, providing complete visibility, maximum security and improved governance of the IT ecosystem.

For example:

- SaaS application permissions defined by the SMP can reinforce the security policies enforced by the CASB.
- Specific SaaS URLs referenced by the SMP can enrich the CASB's knowledge base.
- Data flow control on SaaS applications carried out by the CASB can enhance the SMP's analysis.

SMPs' Role in Discovering SaaS Apps



Together, these two tools establish a solid framework for a secure and optimised SaaS landscape within the organisation. The CASB protects and ensures the application of security policies while enabling precise identification of security vulnerabilities. SMPs, on the other hand, focus on monitoring and analysing the use of SaaS applications (session time, connection frequency, usage retention, length of engagement, pro/perso connection). This enables robust governance to be put in place, encouraging greater collaboration with all stakeholders through collaborative and customisable workflows.

Conclusion

The adoption of SMPs has become a key strategy for large organisations seeking to govern their SaaS landscape and deal with the challenges raised by Shadow IT. Although CASBs play a crucial role in securing and ensuring compliance with access to cloud applications, governance of the SaaS landscape primarily revolves around SMPs. By focusing on the monitoring, management, and control of the usage of these applications, SMPs offer an overview and effective governance over an enterprise's application ecosystem.

*Gartner, Market Guide for SaaS Management Platforms, by:

- February 2021 : Chris Silva, Manjunath Bhat, Dan Wilson, Ryan Stefani
- December 2022 : Andrew Gianni, Andreas Frangou, Austin Steinmetz, Akshay Jhawar

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.

DISCLAIMER: This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from LeanIX. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Beamy

Beamy is the leader in SaaS Management (Software-as-a-Service) for large enterprises, and its clients include major players such as LVMH, BNP Paribas, Decathlon, Axa, and many more.

Large enterprises are facing an explosion in SaaS applications, often implemented by business departments (HR, Marketing, Product) without the knowledge of IT teams. This underground digitisation (or Shadow IT) is systemic and generates major risks for the organisation's security and compliance.

Beamy helps CIOs and IT teams monitor and manage their SaaS ecosystem with confidence, so they can benefit from the democratisation of technology while keeping risks under control.

Using a unique platform tailored to the enterprise's complex and regulated environment, it can automatically and continuously detect and monitor all SaaS used within the organisation, including those in Shadow IT.

Beamy - 32 Rue de Trévise - 75009 Paris

beamy.io

February 2024

The unauthorised reproduction or use of any material protected by copyright or intellectual property rights without express written permission is strictly prohibited. For further information: **marketing.team@beamy.io**