CASB and SaaS Management: Should You Have Both?

Understanding the strengths and weaknesses and finding their place in your security initiative so you can battle Shadow IT

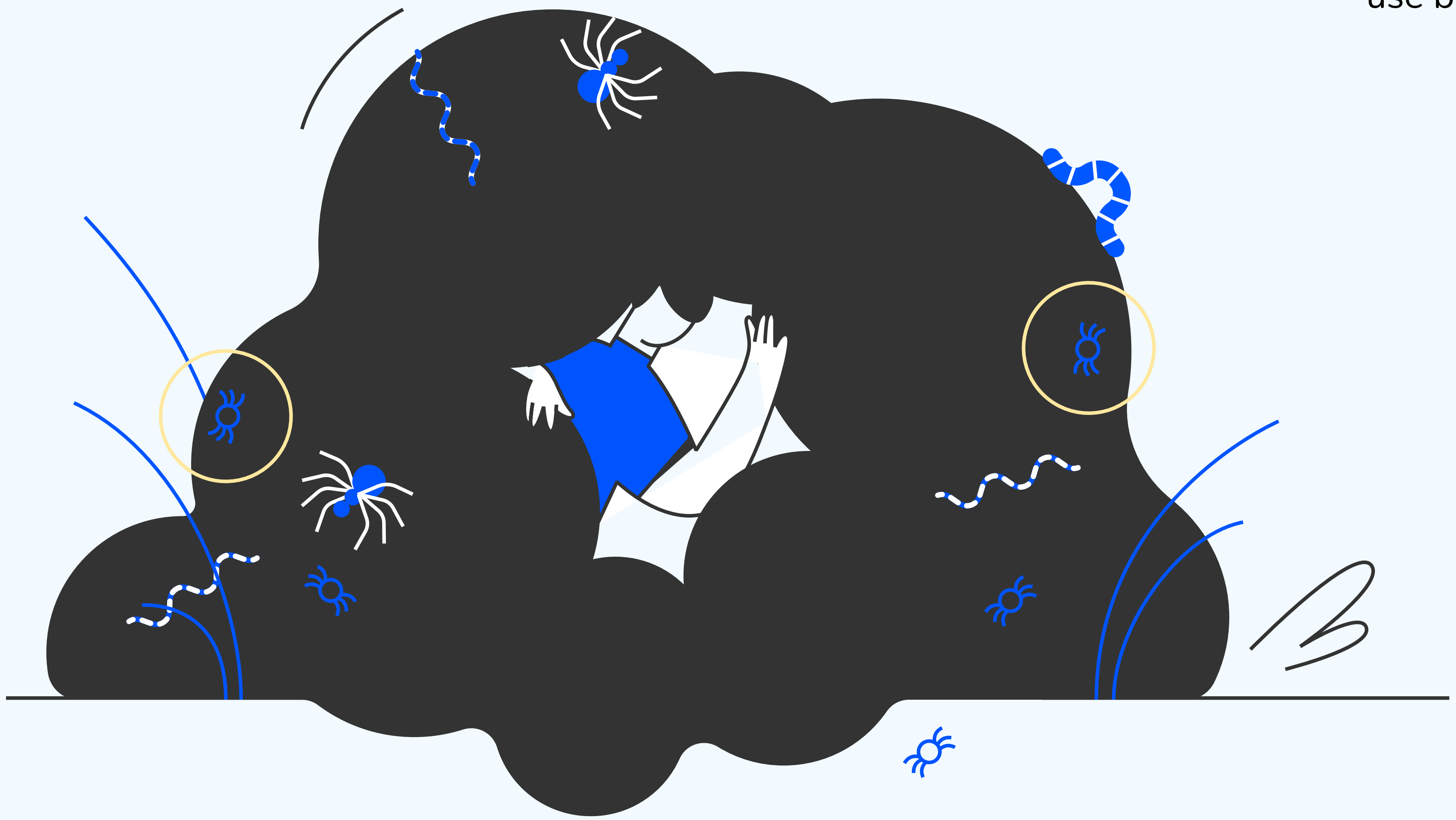
Do you have a grip on Shadow IT in your organization?

Shadow IT is pervasive. It exposes data, it bleeds budgets with hidden costs, and it creates hidden knowledge silos across the organization. However, employees continue to download unsanctioned applications and the cycle continues.

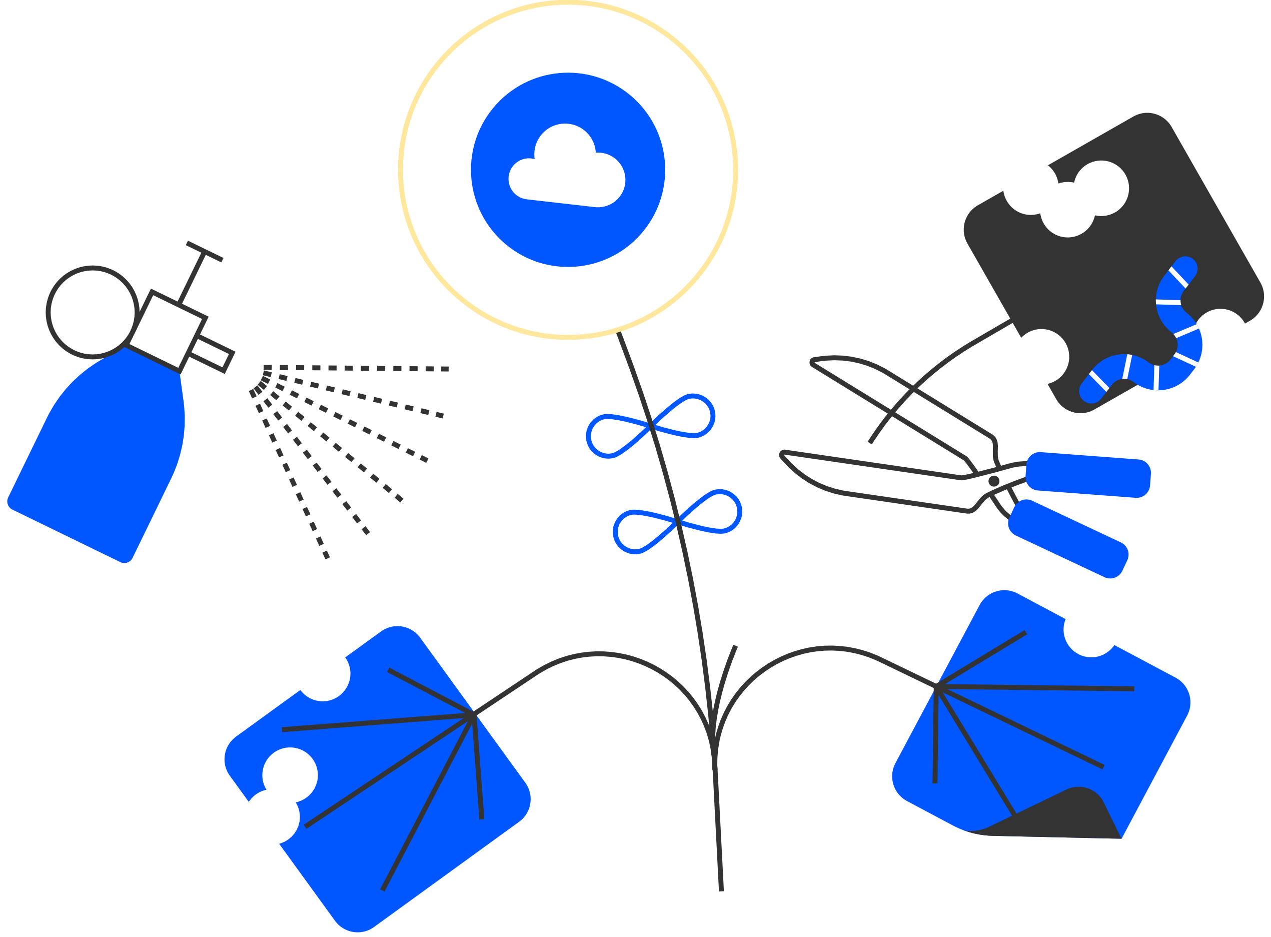
To combat this silent foe, companies and IT teams turned to a set of tools known as Cloud access security brokers, or CASBs, but these tools haven't made Shadow IT disappear.

Now, more and more organizations are considering SaaS Management as another way to fight the spread of Shadow IT.

In this whitepaper, we'll examine the overlaps, the distinctions, and if you should use both.



Introduction



CASB became the de-facto standard for how IT organizations discover Shadow IT in their organizations.

However, as time passed security threats persisted. Instead of software on CDs, employees began downloading their applications through the cloud. Browser extensions became commonplace and the rise of freemium software made the spread of unsanctioned applications uncontrollable.

Companies have begun to look for additional meth ods of containing the threat. Then came the need for SaaS Management.

SaaS management provided a single platform from which IT could oversee and control the infection of their SaaS Swamp - thus providing order and structure to a constantly evolving landscape. **SaaS Management also fills two critical gaps that CASBs have left open:**

Discovery

finding every possible cloud application in the stack.

Action

taking actions such as turning users on/off or migrating data inside of SaaS applications.

This fusion of insight and actionability provided IT teams with a new way to battle the pervasive threat of Shadow IT. With this new solution of SaaS Management, are CASB solutions now obsolete?

Not at all, but to understand, let’s take a deeper look at some of the benefits and limitations inherent to CASB.

What is a CASB?

A Cloud access security broker, or CASB, is cloud-hosted software or on-premises software or hardware that act as an intermediary between users and cloud service providers. CASB's are one of the tools corporate security teams deploy to manage security across software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) platforms.

In addition to providing visibility, CASB solutions allow organizations to extend the reach of security policies into the cloud.

Because of this CASBs have become a vital part of enterprise security, allowing businesses to safely use the cloud while protecting sensitive corporate data.

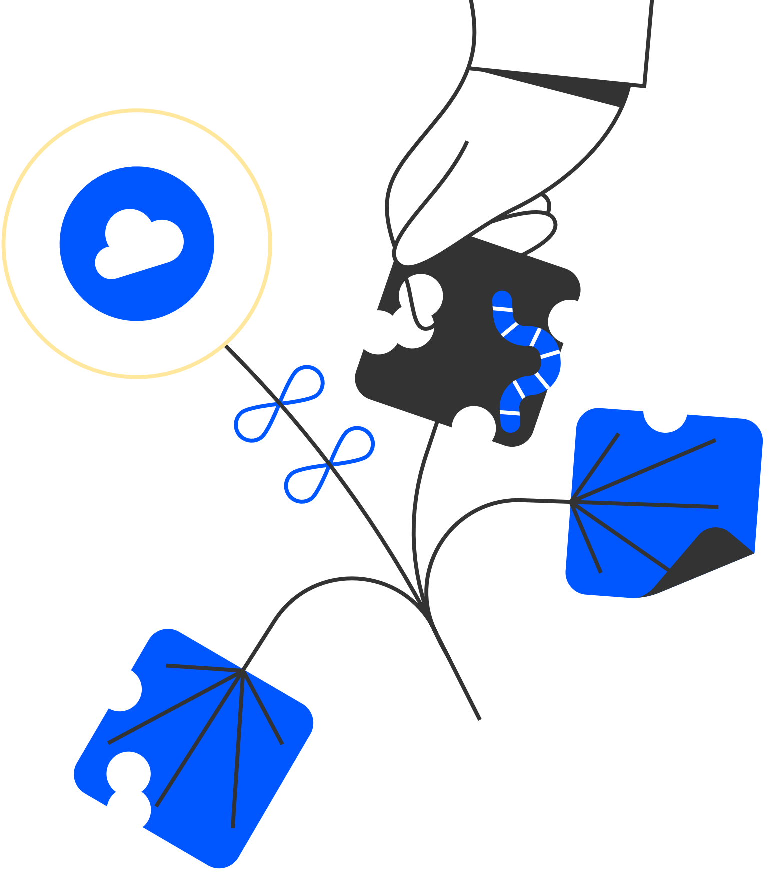
Key Use Cases for CASB

CASB products solve problems related to loss of corporate data, staying compliant with industry standards, and identifying risky user / account behavior that could compromise sensitive data.

Because of this CASB products are heavily focused on being the policy management plane between the enterprise and the cloud. Key use cases include:

- ✓ Actively blocking access to non-sanctioned cloud services.
- ✓ Identify account takeovers
- ✓ Monitor cloud services for risky behaviour
- ✓ Manage configuration settings of cloud platforms
- ✓ Automation of security lifecycle – e.g. integrate with SIEM solutions to pass event data – blocking of a SaaS app, disconnect connect app configurations.
- ✓ Discovery of Shadow IT
- ✓ Monitoring flow of sensitive data so it does not leave sanctioned cloud services. (Cloud DLP)

How CASB and SaaS Management Differ on Shadow IT Discovery



The most obvious area of overlap between SaaS management and CASB solutions is in the area of Shadow IT discovery. Both CASB's and SaaS management solutions will discover applications that are being used in a company that IT and Security teams are likely not aware of. The way in which the two solutions discover Shadow IT, the purpose for which they are built, and who they do it for are quite different.

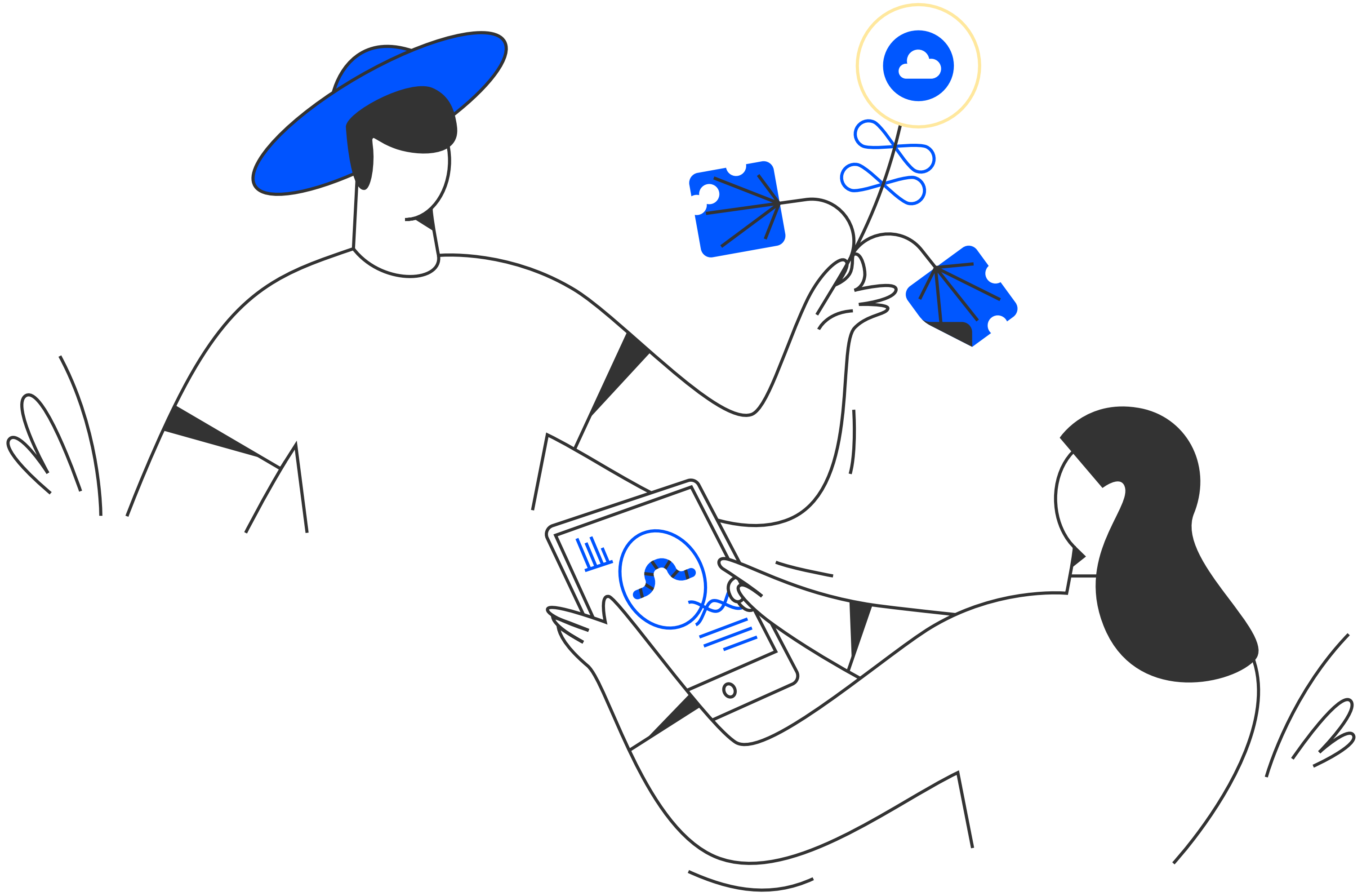
CASB solutions help security teams manage access to cloud apps and data that is stored in those apps to ensure that:

- ✓ Only sanctioned cloud services are used.
- ✓ Data that is stored in the cloud is aligned with information security and data protection policies. (Cloud DLP)
- ✓ Services are continually protected from account takeovers by monitoring for anomalous activity.
- ✓ Services are protected from security breaches due to inadvertent misconfiguration or configuration drift.

SaaS management solutions identify Shadow IT to Corporate IT, procurement and finance so they can save money by:

- ✓ Eliminating redundant applications.
- ✓ Automating workflows related to license management, contracts / renewals, application discovery, and on-boarding / off-boarding.
- ✓ Optimizing usage of underutilized licenses.

Better Together



The technical architecture of both differ significantly with CASB's being far more difficult to deploy with either proxy, agent, and / or API based approaches to deployment. Many products will use a combination of proxy, agent and API to satisfy use cases they support.

SaaS management products are typically very lightweight and will collect data using API's and integration with endpoint technologies such as MDM. As they typically serve a less technical user persona, the setup and integrations are easy to connect in comparison with CASB setups which in most cases require professional services for deployment.

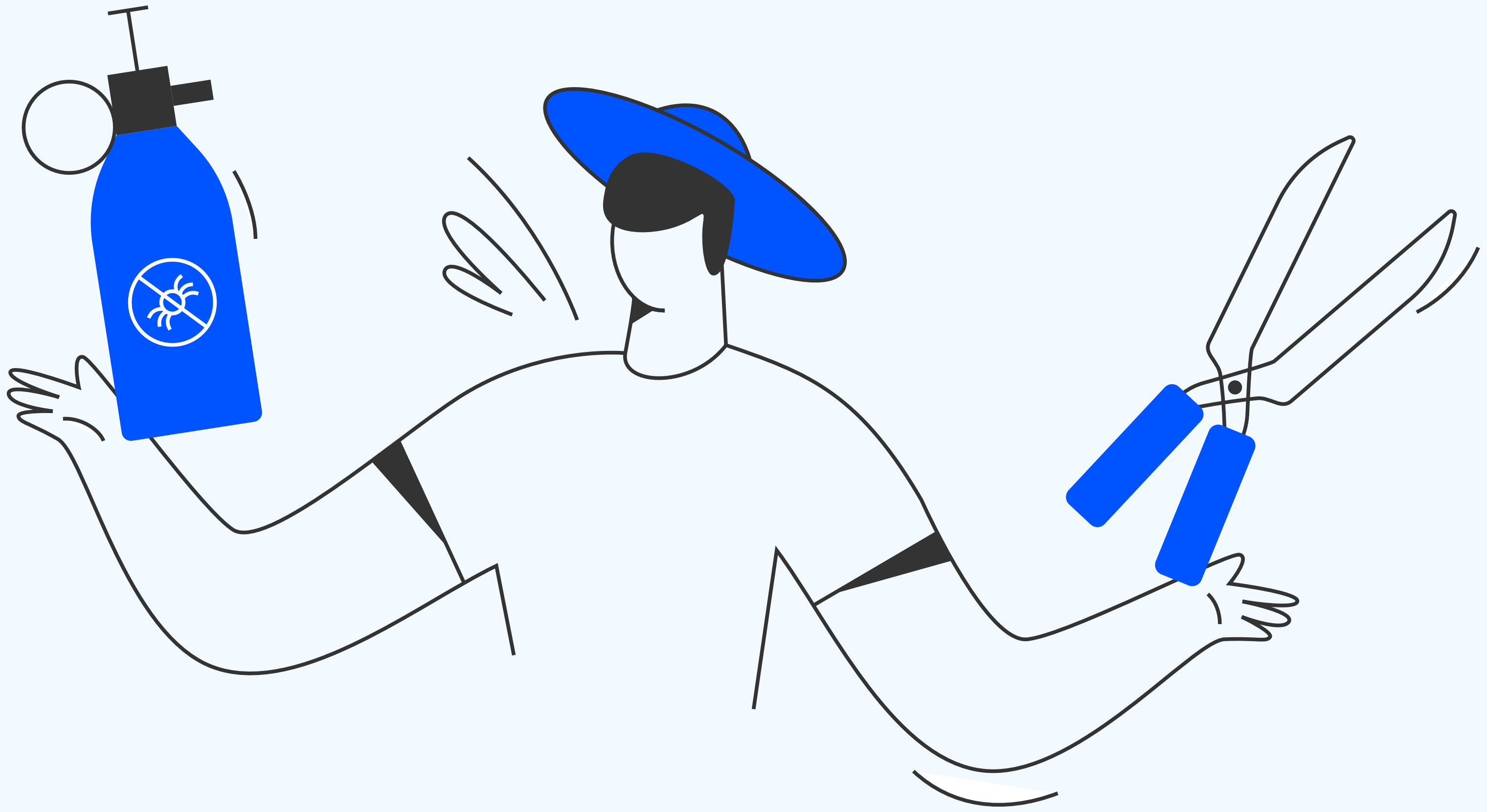
The two solutions can be complimentary as CASB discovered apps can be connected to usage, license, and expense data found in a SaaS management solution. This would allow Corporate IT, Finance, and Procurement teams to leverage the rich discovery capabilities of the CASB to gain even better control of Shadow IT. It would also allow security to leverage the discovery capabilities of the SaaS management solution which typically cover a much broader range of apps through deep API integrations.

Stakeholders across security, IT, finance, and procurement can collectively strengthen their capabilities in Shadow IT discovery and be better positioned to solve their respective business problems:

- ✓ Security gets more high quality data to reduce risk
- ✓ Procurement, finance and IT and finance get more high quality data to save money and optimize operational efficiency.

Conclusion

Should you use CASB, SaaS Management, or both?

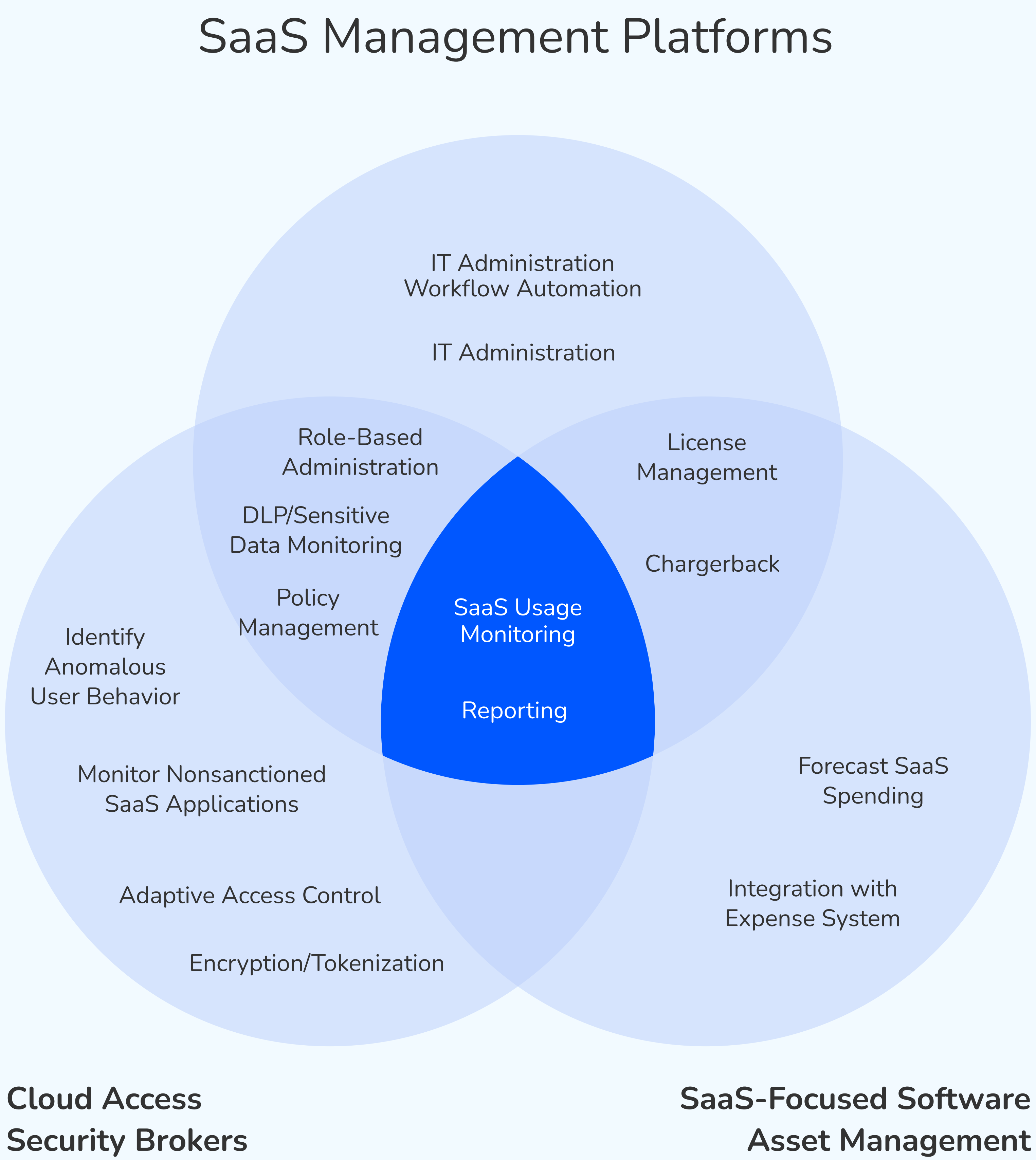


SaaS Management and CASB solutions solve many of the same issues, however they do so in very different ways and for different reasons.

Ultimately, it’s important to understand the requirements within your industry and the capabilities of your team. CASB is excellent for addressing many specific security concerns and corporate use cases. However, the deployment process is much more complex and often the discovery features do not capture the whole picture.

SaaS Management fills these gaps by providing a lightweight method of capturing a more complete picture of the applications within your organization. SaaS Management also provides more opportunities for IT to take action with the insights gained and prevent security risks before they develop.

How SMPs Compare and Contrast with CASBs and SAM Tools


SaaS Management Platforms
IT Administration Workflow Automation
IT Administration
Role-Based Administration
DLP/Sensitive Data Monitoring
Policy Management
License Management
Chargerback
SaaS Usage Monitoring
Reporting
Identify Anomalous User Behavior
Monitor Nonsanctioned SaaS Applications
Adaptive Access Control
Encryption/Tokenization
Forecast SaaS Spending
Integration with Expense System
Cloud Access Security Brokers
SaaS-Focused Software Asset Management

Need Help With Shadow IT Discovery?

Give Torii a try