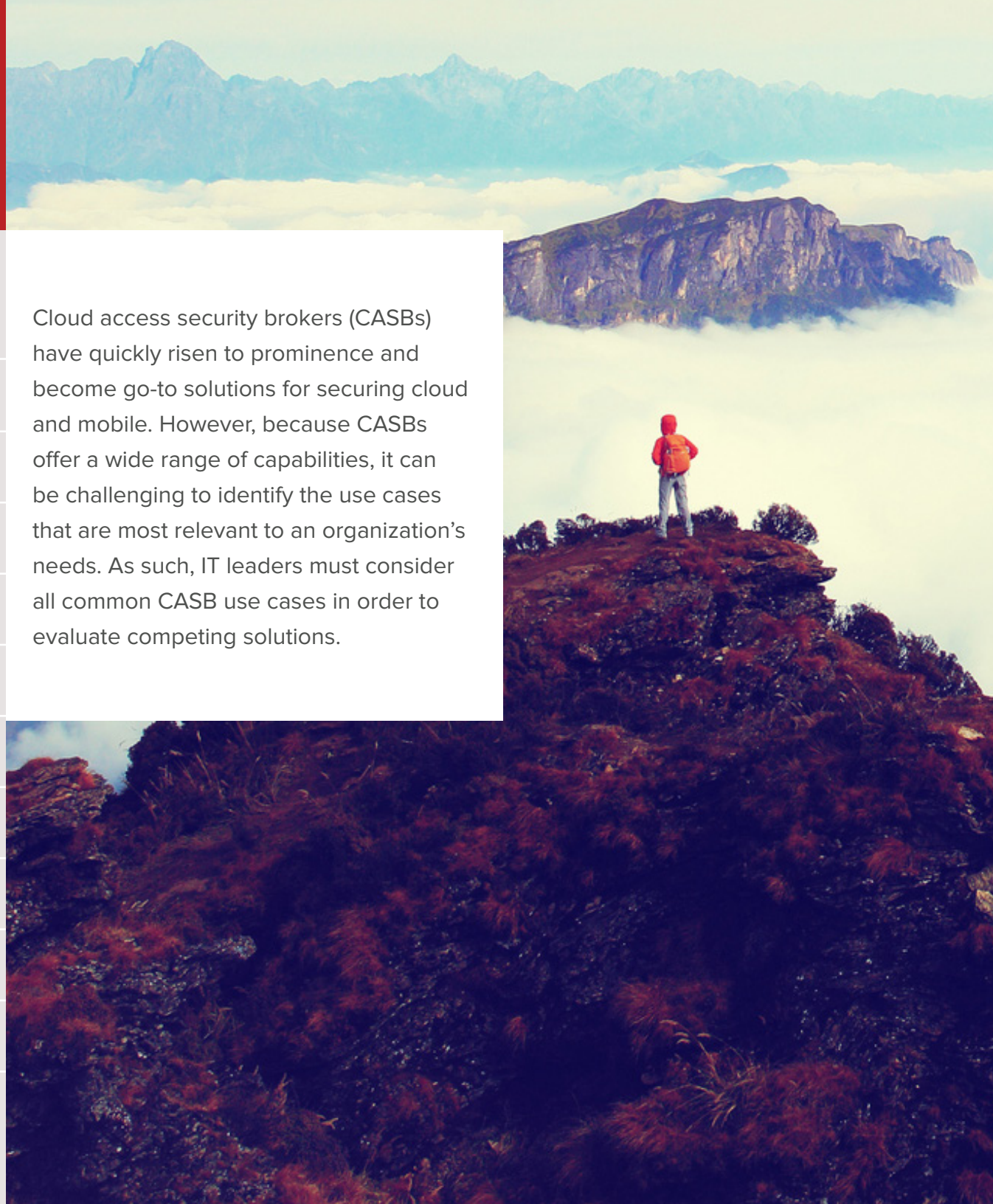
Top CASB Use Cases

bitglass

bitglass

Top CASB Use Cases

Cloud access security brokers (CASBs) have quickly risen to prominence and become go-to solutions for securing cloud and mobile. However, because CASBs offer a wide range of capabilities, it can be challenging to identify the use cases that are most relevant to an organization's needs. As such, IT leaders must consider all common CASB use cases in order to evaluate competing solutions.



Secure Mobile and Personal Device Access

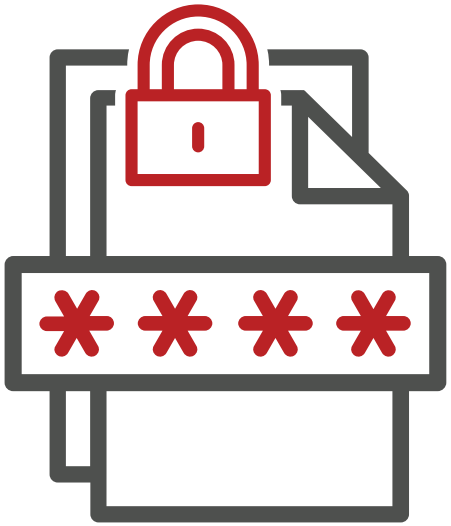
Traditionally, securing mobile devices was done through agents that were installed on managed endpoints. However, as organizations enable bring your own device (BYOD), data is accessed more and more from personally owned mobile devices. When employees use these endpoints for their work, enterprises lose visibility and control over sensitive information. Unfortunately, installing agents and taking control over BYO devices is logistically challenging and is often met with employee pushback over privacy concerns.

Today, organizations need to adopt CASBs with agentless mobile data protection capabilities. These CASBs offer access controls that can allow, limit, or block access to unmanaged and mobile devices. This control over the flow of data is paired with an ability to set device security configurations, such as requiring the use of PIN codes rather than swipe patterns. Finally, with the click of a button, selective wipe can target and delete corporate data on unmanaged mobile devices without harming personal data. With an agentless CASB, this can all be done without requiring the installation of agents.

Prevent Data Loss with DLP

Data loss is a major concern for any organization migrating to the public cloud. Applications like Office 365, G Suite, and Dropbox are built to enable simple sharing and collaboration. While this provides a great deal of productivity, it also exposes organizations to the potential for data leakage. As such, data loss prevention (DLP) is a must for any organization using cloud-based services.

CASBs provide a variety of DLP capabilities. An enterprise can leverage DLP to redact sensitive information in emails, watermark documents for tracking, apply DRM to files to require additional authentication, and more. Additionally, CASBs can integrate with existing, premises-based policies in order to ensure the consistent protection of data.



Limit Risky External Sharing

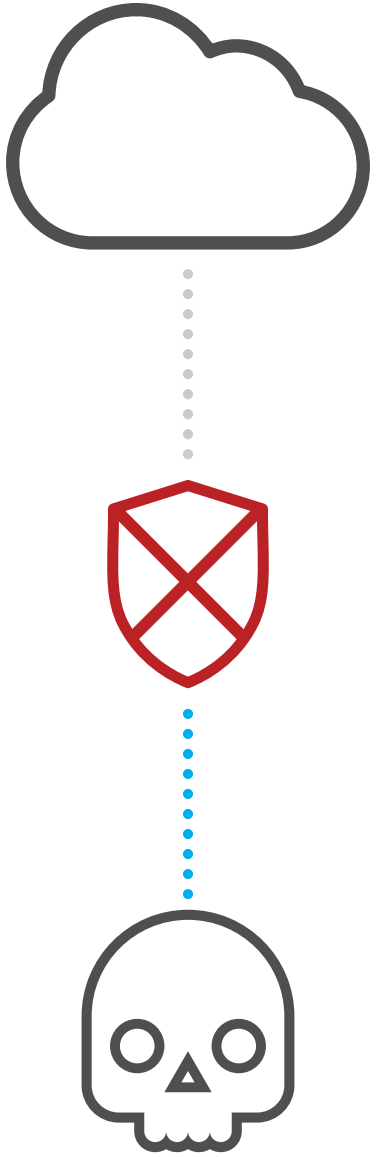
One of the cloud's greatest benefits is simple, rapid sharing and collaboration. However, while cloud apps enable efficiency and teamwork, they may expose the company to data leakage risk. Whether an employee carries malicious intent or is simply careless, corporate information may be shared with individuals outside of the organization.

Sharing controls are provided by most CASBs. They can scan apps like Google Drive to search for external shares and revoke them accordingly. Access controls can be configured to deny access to personal email addresses, unmanaged devices, users who aren't on premises, and more. Finally, DLP policies like watermarking can be used to track files as they are downloaded by unauthorized users.

Stop Cloud Malware and Ransomware

Outbreaks like that of the WannaCry ransomware in 2017 are clear examples of why organizations need malware protection. Because of cloud and BYOD, threats now have more attack surfaces for infecting organizations. A single contaminated file uploaded to the cloud can quickly spread throughout an entire enterprise if it is downloaded to other devices or if it infects a connected app. Unfortunately, the majority of cloud applications don't provide any built-in malware protection, leaving it to the enterprise to risk their security or deploy a third-party solution that extends native cloud capabilities.

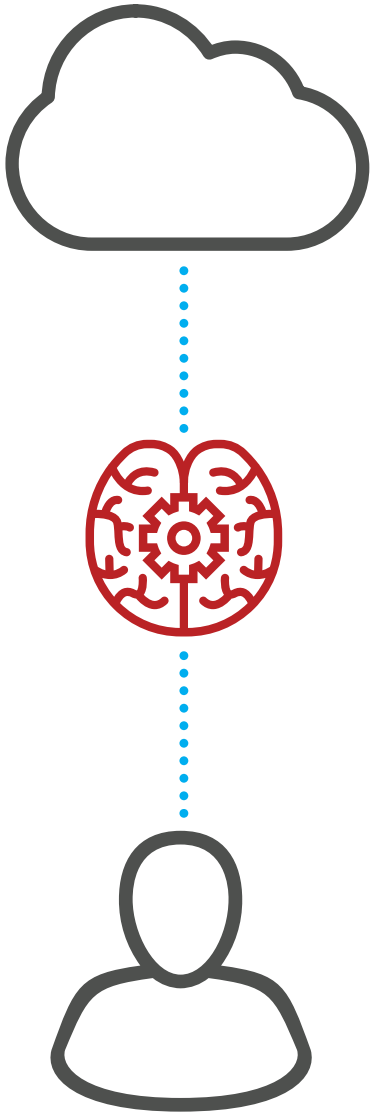
CASBs with advanced threat protection (ATP) leverage the latest machine-learning-based techniques to defend against both known and zero-day malware. CASBs leverage inline proxies to stop the flow of malware from devices into the cloud. At the same time, they leverage API-based connections to scan for malware-at-rest, preventing it from being downloaded to other devices and spreading to connected cloud applications.



UEBA and Cross-App Visibility

Employees can store corporate files in a variety of cloud apps that enable collaboration. This complex web of user and file accesses across multiple applications poses a challenge to organizations that need to monitor corporate data and distinguish legitimate data accesses from those that are rogue or malicious.

CASBs address this challenge through a combination of detailed activity logs and user and entity behavior analytics (UEBA). With logs that enable audit, individual files and users are monitored in a way that grants administrators comprehensive, cross-app visibility. A CASB with UEBA leverages this cross-app visibility to analyze behaviors and take corrective actions in real time. For example, if a user accesses Salesforce from Russia five minutes after logging in to Office 365 from California, a CASB can detect the anomaly and enforce step-up, multi-factor authentication (MFA).



Encrypt Data-at-Rest

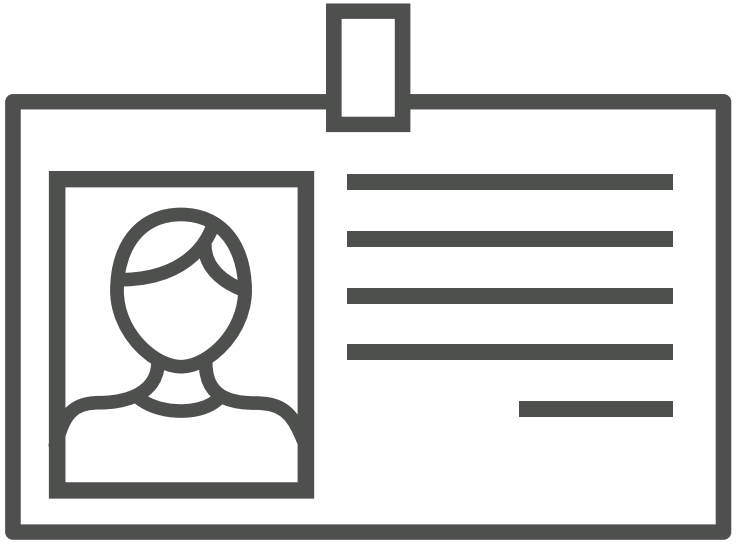
Some organizations have policies or regulatory mandates that require them to protect and control their data everywhere—including when it moves to the public cloud. These firms must take steps to obfuscate data stored in cloud apps. Unfortunately, native cloud app encryption typically allows cloud app vendors to see encrypted data. Additionally, many third party encryption solutions either break key application functions like search and sort or weaken encryption to allow said functionality.

With next-gen CASB encryption, corporate data in the cloud can be protected from unauthorized users. By providing organizations with control of their own encryption keys, CASBs can even shield against the eyes of the cloud app vendors who store encrypted files. Field-level data in applications like Salesforce and ServiceNow can also be encrypted in the same fashion; however, organizations must select CASBs that offer full strength encryption that does not reduce the usability of data.

Securely Authenticate Users

Identity and access management is a core component of a fully integrated CASB solution. Enterprises need to verify users' identities when they log in to cloud applications that contain sensitive corporate data—particularly when that data is regulated. This goes beyond enforcing complex passwords; organizations need visibility into logins and control over user access to applications.

CASB identity capabilities have greatly evolved, obviating the need for a dedicated IDaaS solution. Today's leading CASBs feature built-in group and user management via Active Directory, single-sign on across all applications, and native multi-factor authentication (MFA). With a CASB, organizations can log all authentication attempts, step up to MFA in risky contexts, and provision users with ease.

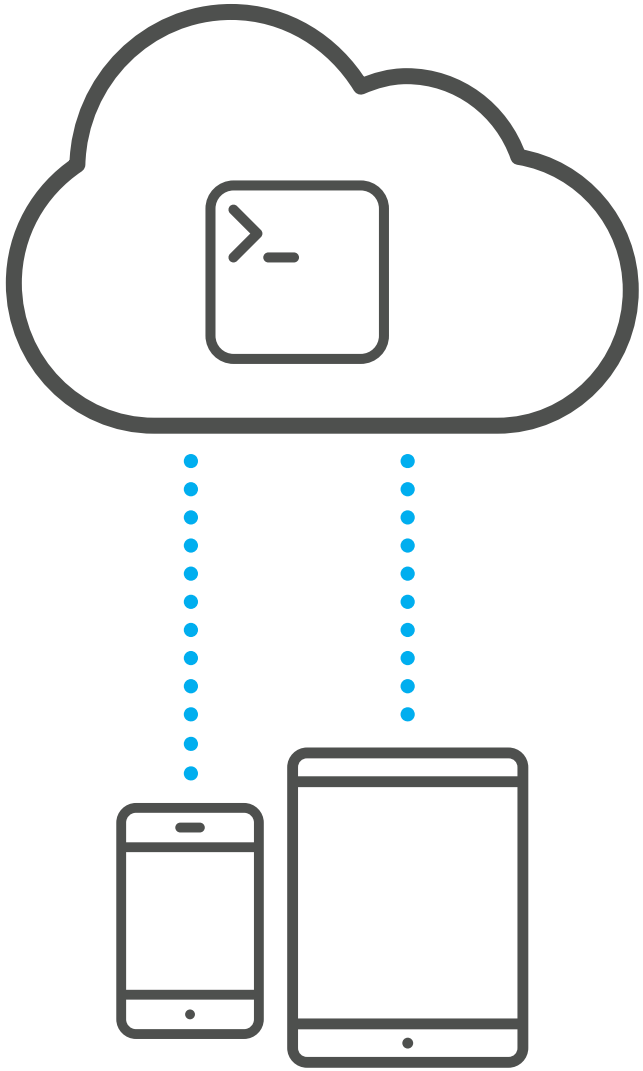


Secure IaaS and Perform CSPM

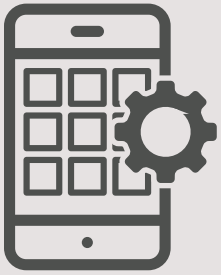
Infrastructure-as-a-service (IaaS) offerings like AWS, Azure, and GCP grant organizations the power and flexibility of the public cloud, but with more control over the underlying infrastructure. Naturally, this increased control also comes with a greater responsibility for security.

Fortunately, leading CASBs are equipped with the capabilities needed to secure IaaS environments. Storage services like Amazon's S3 can be scanned for sensitive data-at-rest, custom applications can have files and field-level data encrypted, and both can be secured via data loss prevention (DLP). Additionally, contextual access control and multi-factor authentication can be used to defend IaaS management consoles.

Cloud security posture management (CSPM) is another critical CASB capability. CSPM functionality scans IaaS instances for misconfigurations that could yield data leakage or noncompliance with regulatory demands. Leading CASBs can detect misconfigurations as defined by various benchmarks like CIS, PCI DSS, and HIPAA, and remediate automatically.



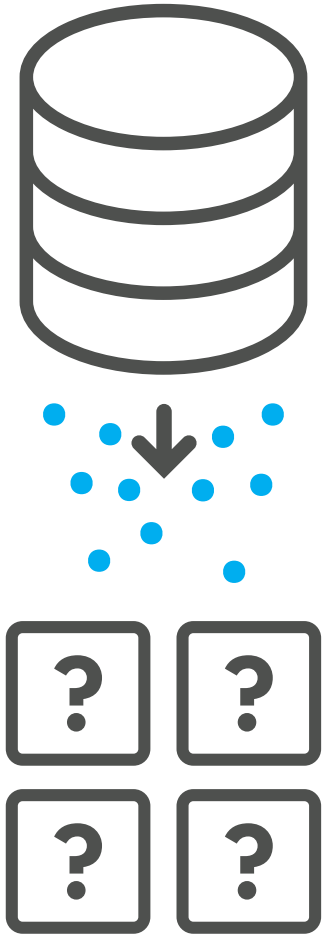
Control Unmanaged App Usage



Unmanaged cloud applications are a large threat to security in the enterprise. Shadow IT, as these apps are called, occurs when employees store and process corporate data in cloud applications that are not sanctioned by IT. Losing visibility and control of data in this way can lead to extensive data exfiltration and, consequently, reputational and financial losses.

With a CASB, users who try to access unmanaged cloud applications for corporate purposes can be detected in real time. While some organizations may block any such app, others prefer a less heavy-handed approach. Through coaching, users are notified in real time that the app they are attempting to access is unsanctioned and are then provided with a sanctioned alternative—either with or without blocking the unmanaged app.

Leading CASBs can also enable controlled access to unmanaged apps by making them read only. In this way, the enterprise can prevent data leakage events such as the upload of sensitive information to one of these applications. This is particularly helpful given the variety of apps that employees may need to access in the course of working with partners, suppliers, and others.



Top CASB Use Cases

When using dozens of cloud applications and countless devices, traditional security solutions are no longer adequate. Organizations need a comprehensive CASB that offers data protection, threat protection, identity management, and visibility. Only Bitglass provides agentless, real-time security on any app, any device, anywhere. Request a free trial to take the first step towards securing your data.

bitglass