Lookout®

Evaluating Cloud Access Security Brokers

CASB BUYER'S GUIDE

Contents

Unprecedented Life in the Cloud

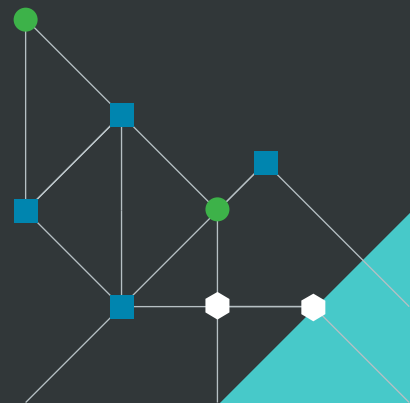
Prior to the pandemic, most organizations had started on the path to digital transformation. Then, 2020 came crashing down on IT teams. Changes forced data and users to the cloud, and accelerated digital transformation in unprecedented ways.

As employees left the confines of their offices, so too did the status quo of accessing data from managed or corporate-issued devices within the network perimeter. Instead, for many, unmanaged devices became the primary method of accessing data in order to stay productive. Companies with tens of thousands of employees now had the same amount of home networks accessing the corporate network. And VPNs were overburdened and unable to keep up with the sprawling demand they were never designed or implemented for.

IT and security teams lost visibility and control when the world went home.

1. Users circumvented VPNs and directly connected to cloud applications
2. Unsanctioned application usage increased to support productivity
3. VPNs made it nearly impossible to implement zero trust
4. Dangers of data loss increased with diminished control
5. Direct connection and inability to apply access policies created opportunity for dangerous lateral movement

Companies embracing remote work and cloud as they shifted to accommodate the increasingly online world faced costlier data breaches. Nearly 20% of organizations studied by Ponemon reported that remote work was a factor in a data breach. And, breaches ended up costing companies $4.95 million – an increase of nearly 15% from the average breach.[1]



[1] https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

Cloud Access Security Brokers Explained

Cloud Access Security Brokers (CASBs) quickly became an essential element of cloud security strategies across all organizations facing the effects of remote work. Designed to address security gaps created by distributed workforces connecting from managed and unmanaged devices, CASBs deliver cloud-specific security capabilities that traditional perimeter-focused products can't.

Because of its unique capabilities, CASB's growth remains higher than any other technology in the information security market.

CASB investment ballooned by **41.2%** since 2020

– 2021 CIO Agenda Survey[2]

4 Pillars of CASB

Visibility

Granular visibility and control across cloud applications, users, data, devices, and user activity to identify cloud usage, cloud data repositories, risky clouds and users, and unsanctioned cloud utilization.

Data Security

Powerful data protection controls to identify, classify and secure sensitive cloud data, along with integrated data encryption, masking, redaction, removal, and prevention of external users or domains from accessing shared folders.

Threat Protection

Antivirus and anti-malware integration for deep scanning of all incoming and outgoing traffic for malicious content or infected files, along with User and Entity Behavior Analytics (UEBA) to identify anomalous user behavior in real-time and prevent potential data breaches related to bad actors and internal threats.

Compliance

Centralized compliance with data protection laws (GDPR, HIPAA, CCPA, GLBA, SOX and more) with data privacy and localization requirements.

[2] https://www.gartner.com/en/information-technology/insights/cio-agenda

CASB Deployments: Methods for Every Environment

When evaluating CASB options, there are often two modes of operation to choose from – proxy-based and API-based. Understanding the differences is a critical step when aligning solutions with the exact needs of your organization.

Proxy-based CASB

Proxy-based deployments mean the CASB sits between the organization and cloud applications to control the flow of data through a single gateway in real time. Doing this ensures that the data always travels to the cloud in a protected form.

Proxy-based deployments are offered in two models:

- **Forward proxy:** CASB in forward proxy mode routes all traffic from endpoint to the CASB instance. It can either work with existing proxy services that can forward traffic to CASB proxy, or it will need an agent software installed on managed devices to forward traffic to the CASB.
- **Reverse proxy:** CASB in reverse proxy mode provides secure agentless connectivity for all devices, including mobile and unmanaged devices. It works by simply redirecting all traffic through the CASB to the service provider.

Proxy-mode advantages: Flexibility.
Proxy-mode challenges: Potential performance issues, architectural issues of where to host the CASB, and how TLS sessions are handled.

API-based CASB

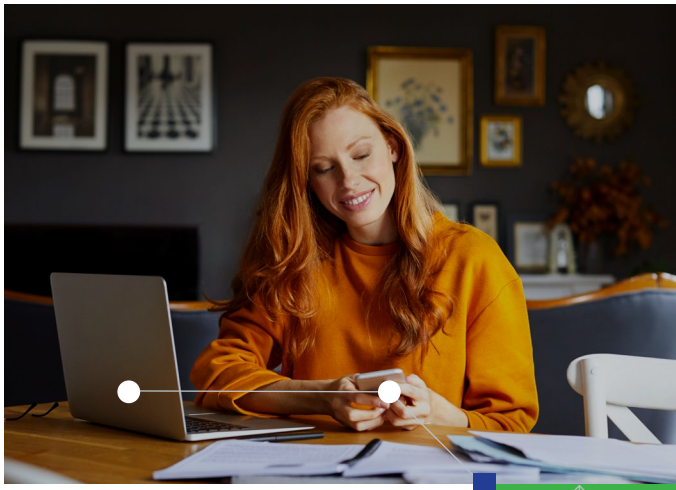
API-based CASB is an out-of-band solution that does not sit in the direct path between the organization and the cloud applications. This deployment method provides deep data visibility and enforces data protection policies via an API trigger after the data gets uploaded to the cloud. Since the operation is asynchronous, there is no performance impact or latency in user experience. API mode provides coverage across both managed and unmanaged devices, with data protection using data loss prevention (DLP), data discovery, classification, posture management, audit trails, user activity monitoring, content inspection, scanning user privileges, sharing permission on files, folders, and app security settings.

API-mode advantages: Does not have TLS and session management issues.
API-mode challenges: APIs developed and exposed by SaaS providers are specific to unique service offering.

Given the complexity of today's hybrid environment, many organizations may need a blend of the different deployment modes. In this case, it is advisable to find a CASB that can be deployed in all methods.

CASB Pillar: Visibility

Data leakage in the cloud is a top concern for every organization and creates a greater need for CASB, which maintains visibility over data that resides beyond the perimeter of on-premises tools. While all CASBs offer some form of visibility, there are three main functions that forward-looking solutions will include:



- **Activity logs:** CASBs should integrate with all existing security logs from network devices, firewalls, and proxy services with the goal of gaining full visibility and knowledge of how sensitive data is being used. Using a CASB, organizations will have detailed logs on all cloud transactions including, logins, uploads, and downloads, as well as, application-specific behaviors (external file sharing, etc.). Using this in-depth detail, organizations know not only where data resides, but how it is being used, by which users, on which devices, and geo locations.
- **Shadow IT discovery & assessment:** Using activity logs, CASBs should have the capabilities to discover shadow IT, also known as unsanctioned applications, and manage or block access. Less sophisticated CASBs do this through manual detection and cataloging of unsanctioned cloud applications. Comparatively, adept CASBs leverage machine learning for automated detection, analysis, and classification of shadow IT for faster visibility and control in real time.
- **Cloud Security Posture Management (CSPM):** As organizations migrate their business critical applications to the cloud, many struggle with automating their security posture across multiple SaaS and IaaS clouds. Without a simple way to do this, misconfigurations and user errors occur. When selecting a CASB, it is imperative that it includes CSPM to perform automated assessments of cloud landscapes against well-defined security and compliance guidelines. This allows organizations to identify anomalies and remediate implementation issues to prevent breaches. For easy monitoring and control, these features should be accessible through a centralized dashboard with drill-down functionality to reduce operational complexity.

CASB Pillar: Data Security

Many CASB solutions today only address data as it is being shared to the cloud, rather than offering end-to-end protection. As multi-cloud adoption rises and the popularity of policies like BYOD introduces masses of unmanaged devices, organizations will require a CASB that can keep pace with the evolving scope. There is now a greater need for a single environment to oversee data security across SaaS, PaaS, and IaaS accounts without operational complexity.

Most companies are now storing highly sensitive data on their public cloud applications – requiring cloud encryption to protect data in motion and at rest. First-generation CASB solutions often do not offer encryption or only do so when data is at rest, which is no longer enough to protect cloud data from attackers.

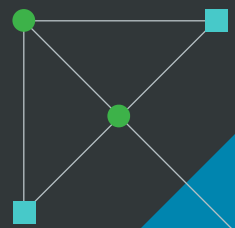
Protect your data wherever it resides with integrated DLP

Consistently manage data across multiple SaaS applications, emails and custom cloud deployments, and ensure the security of sensitive information through extensive data protection options that go beyond basic allow/deny capabilities.

Questions to consider when reviewing CASB offerings:

- Does it have multi-mode data inspection for securing historical data and real-time cloud collaboration?
- Does it have context-aware policy enforcement such as upload, download, share, and collaborate?
- Are there predefined and customized policy templates to address regulations such as PCI, HIPAA, and GDPR?
- Does it use advanced file and image scanning?
- Does it integrate with enterprise DLP systems to extend corporate policies to cloud applications?

Granular and policy-based data protection ensures all data is protected, in every scenario.



CASB Pillar: Threat Protection

As organizations expand their cloud use, it is imperative that the platform does not become a channel for malware delivery to their users and internal networks. To proactively protect, selecting a CASB that uses comprehensive defenses including signature-based detection and behavior-based protection is key.

Signature-based vs. Behavior-based

- Signature-based protection relies on accessing an extensive catalog of malware signatures to identify and block any malicious attempts.
- Behavior-based protection uses continuous monitoring of activities by users, devices, and applications to detect anomalous behavior.

Integrated User and Entity Behavior Analytics (UEBA)

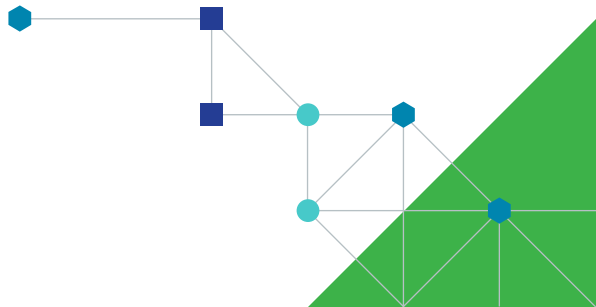
CASBs with integrated UEBA can offer the greatest behavior-based protection to prevent data leaks and losses from compromised accounts:

- Uses machine learning algorithms to model the behavior of users and devices on cloud apps, then detects deviations from normal behavior patterns and highlights anomalies that could be a sign of cyberattack.
- Monitors user and entity activities on a real-time dashboard and offers click incident analysis.
- Details geo-logins, source IP addresses, and devices used.
- Provides specifics on user behavior such as content uploads and downloads, edits, deletes, logins, and logouts.

Handling potential threats

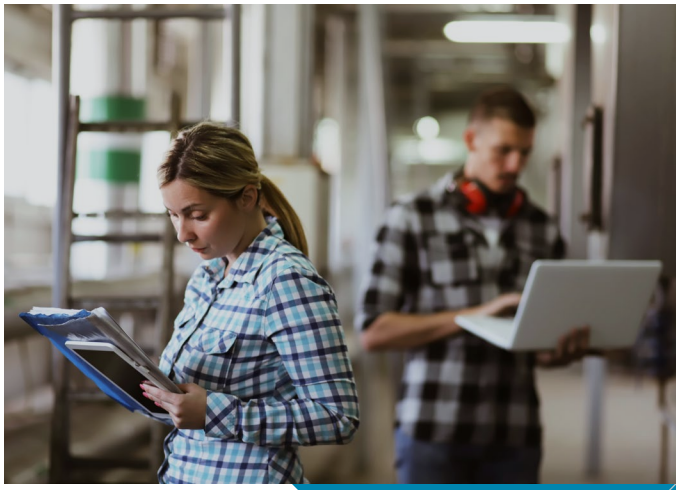
Equally as important as detection is how a CASB handles a potential threat. Consider a solution that offers zero-day threat protection and sandboxing. With this feature, you will be able to scan all inbound and outbound cloud content for malicious code, and clean or quarantine infected content in real time without adding latency.

UEBA uncovers large numbers of downloads from an individual user, higher than normal logins from the same user, persistent login attempts from the same user.



CASB Pillar: Compliance

Relying on cloud providers to meet compliance requirements is not sufficient for the growing body of regulations. While organizations in industries such as healthcare and finance are used to meeting stringent standards, regulations such as GDPR are starting to encompass a larger swath of businesses. Selecting a CASB that makes it easy to comply and report on compliance is a critical component in future-proofing business.



Questions to ask about CASB governance and compliance:

- Are there predefined templates that enable the organization to migrate to the cloud in alignment with data privacy regulations across the globe?
- Is there an encryption and key management architecture that enables cloud applications to selectively encrypt data for each required country?
- Are encryption keys exclusively retained by the organization and not shared externally with the cloud service providers?
- Does it offer "safe harbor" exemptions to the breach notification laws?
- Can it perform historical scanning of existing data across multiple SaaS clouds, enabling comprehensive data audits?
- Does it come standard with out-of-the-box DLP templates to identify security blind spots, detect open shares, and address global regulations?

Automate security posture to meet compliance requirements

CSPM and SaaS Security Posture Management (SSPM) perform automated assessments of cloud landscapes against well-defined security and compliance guidelines. Given that most organizations now use a variety of SaaS and IaaS clouds such as Office 365, Box, Salesforce, AWS, and Azure, CSPM and SSPM make it easy to gain a comprehensive view of the entire cloud risk posture through a centralized dashboard. By choosing a CASB with this feature, you will not only reduce operational complexity, but you will also be able to prevent data loss from misconfigurations and ensure your multi-cloud infrastructure adheres to the latest compliance guidelines.

Our Mobile World Requires a Mobile-Friendly CASB

From a productivity perspective, BYOD policies are winning – in fact, companies with a BYOD policy gain an extra 240 hours of work per year.[3]

Due to the increasing prevalence of mobile devices accessing cloud environments, it brings into focus the necessity of CASB solutions integrating mobile defense into all four pillars.

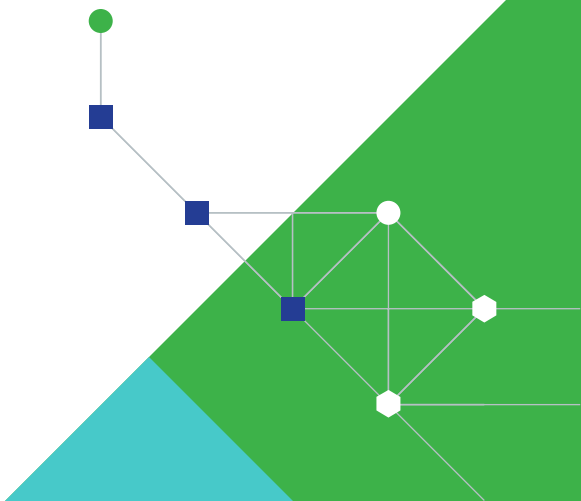
The importance of agentless deployments in a BYOD world

To ensure that mobile devices are included in the protection that CASB solutions provide, agentless deployments are the first requirement. With agentless deployments, the CASB does not require software or certificates to install on devices. That means, if an employee uses their own smartphone, IT and security teams do not have to manage the device in order to protect. The user simply sets up their applications as they normally would and it automatically configures and communicates with the proxy.

Mobile Threat Defense (MTD) integration

When evaluating CASBs, look for offerings that integrate an MTD solution to reduce the amount of siloed management needed. With MTD, security teams can provide the risk status of mobile devices and block the connection to an organization's resources based on that status. It also adds more contextual signals and data points for policy creation and enforcement. The MTD in use should work equally well for both managed and unmanaged devices for comprehensive protection.

Employees access an average of **5.2** mobile business applications daily.[4]



[3] https://techjury.net/blog/byod/

[4] Ibid.

CASB Charts the Path Towards Security Service Edge (SSE)

Securing access to data, from any user, using any device, and from any location is the big picture goal for organizations navigating the hybrid workplace. To do this, Gartner has introduced the Security Service Edge (SSE) – a unification of security services, including Secure Web Gateway (SWG), CASB, and Zero Trust Network Access (ZTNA) to secure access to web, cloud services, and private applications.

When seeking out the ideal CASB, consider looking into the future. Take into account the capabilities as well as how it integrates with the larger SSE environment.

ZTNA

Aimed at solving the complexity of siloed security measures, SSE enables a 360-degree view from the edge to the cloud. As part of this, CASBs must pair with ZTNA solutions to offer adaptive, identity-aware access to applications hosted on-premises and in the cloud.

ZTNA differentiators:

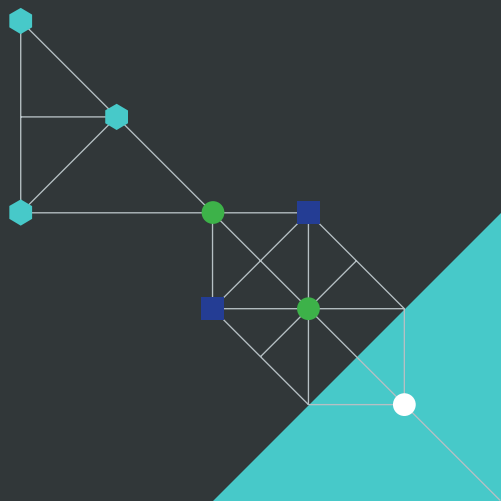
- ZTNA protects on-premises/private applications and infrastructure.
- ZTNA provides segmented access, which is safer than the all-or-nothing access approach of VPN.

When combining these features and CASB in a single integrated platform, organizations can ensure uniform data protection policies across the board.

SWG

Moving forward, CASB and SWG will more often than not be in the same conversation. While both are proxies, they serve distinctive purposes and have the potential for replacing next-generation firewalls (NGFW). Where CASBs offer greater control over traffic as it travels to any device – managed or unmanaged – SWGs can provide monitoring and management for managed devices and corporate networks. When evaluating CASBs, consider that one of the main goals of SSE is to reduce the number of vendors an organization requires for a strong security posture. Organizations that narrow down vendors that offer both functionalities will find it easier to adopt an SSE framework.

SSE is the next framework to guide organizations in the neverending quest to reduce complexity, costs, and vendor sprawl.



Reclaim Control with Lookout CASB

For over a decade, Lookout has been securing cloud information across the widest range of clouds – SaaS, PaaS, IaaS – and with visibility and control over all users and devices, including mobile. With Lookout CASB, organizations gain the greatest depth and breadth of product capabilities:

- Frictionless deployment for cloud applications
- Agentless design for rapid deployment
- Zero Trust adaptive access control
- Integrated UEBA
- Cloud and SaaS Security Posture Management
- Integrated Secure Email Gateway with advanced DLP
- Advanced policy engine and compliance management
- Advanced data protection (data discovery, data loss prevention, enterprise digital rights management, and encryption)

Uncover shadow IT like never before

Unmanaged devices and clouds are no longer an uncontrollable risk. Lookout CASB protects against known devices and cloud applications, and shadow IT – all delivered through an intuitive in-depth dashboard with real-time alerts and audit reporting.

- Identifies nearly 20,000 applications
- Completes risk analysis based on ~60 attributes per application
- Provides insights and risk scores based on users, clouds, application categories, data transfer, and cloud 'risk'
- Generates proxy rules to block/allow cloud applications based on risk and policy
- Supports all major enterprise proxies

Powerful telemetry for informed actions

- 200M+ devices analyzed
- 160M+ apps analyzed
- 4B+ URLs analyzed
- 1,200+ unique malware families found

Unparalleled telemetry empowers organizations to make the data-driven decisions they need to make quantifiable change in protection. Combining native threat intelligence, third-party threat intelligence, and machine learning, the Lookout CASB can detect and stop unauthorized users, malware, and ransomware in all inbound and outbound content. When malicious activity occurs, Lookout automatically quarantines infected content on the fly without latency to ensure protection while maintaining a seamless user experience.

Lookout®

As security and threats continue to change, take control of your digital future with Lookout CASB.
To learn more, request a demo at **lookout.com/contact/request-a-demo**