FORTRA

Protect Your Cloud Data:

The 5 CASB Use Cases You Can't Ignore

The ultimate test for CASBs: Protecting data

Cloud migration has transformed business operations, elevating SaaS apps like Microsoft 365, Google Workspace, and Salesforce to critical infrastructure status. But with the majority of your data and apps now residing in the cloud, the perimeter-based security tools you relied on are no longer effective.

To protect your data and the hybrid workforce accessing it, you need a solution built for the cloud — a cloud access security broker (CASB). But all CASB products are built differently; many of them only focus on the data within SaaS apps and don't extend protection beyond those platforms.

Fortra's data-centric approach

As you search for the right CASB, you might be tempted to focus on technical capabilities. Our approach to cloud security focuses on data. We believe a CASB should function as a cloud-native data loss prevention (DLP) solution, ensuring that data remains protected —whether it's inside SaaS apps or flowing to apps and devices that your organization doesn't control.

Here are five real-world data protection use cases your CASB should beable to handle.

USE CASE 1

Protecting Data Shared With Partners and Contractors

Protecting Data Shared With Thousands of Contractors

A leading construction firm used CASB keep sensitive data safe while making it accessible to its network of contractors. See how they did it.

READ CASE STUDY ›

The cloud has made sharing data easy, even to third parties that have their own devices and apps. But with sensitive information flowing to places your IT teams don't control, your existing security policies have become ineffective. One way to protect data is to simply lock down access, but that severely hinders collaboration that you've gained by using cloud services.

Extend protection beyond your apps

To enable collaboration while protecting data, you need to classify and apply data protection policies in real time, including moments when sensitive information leaves your organization.

- **Apply selective restrictions to individual files:** Rather than deny access altogether, you should be able to enforce more dynamic policies such as making data "view-only," watermarking documents with disclaimers, or masking or redacting keywords.
- **Encrypt data with time limits:** Another way to protect data outside your SaaS apps is to encrypt it as it's being downloaded or shared. By setting a time limit, you can request step-up authentication or require the use of managed devices. And, of course, you limit access.

USE CASE 2

Safeguarding Data Shared Via Email

FinServ Firm Migrates Email Services to the Cloud With Confidence

Discover how a finance institution trusted CASB for data protection as it migrated its email service to the cloud.

READ CASE STUDY ›

Emails frequently contain a wealth of sensitive information — from corporate data and trade secrets to financial specifics and data protected by regulatory mandates.

Despite this, CASB products often don't protect cloud-based apps like Google Gmail and Microsoft Outlook. This forces organizations to look for separate, dedicated solutions for email security.

Detect and protect sensitive data in emails

As the cloud makes security management more complex, it's important to enforce the policies you've designed for SaaS apps and apply them to email services.

- **Detect sensitive data regardless of format:** Discover sensitive data, whether it's within the body of the email or inside an attachment, including zip files, spreadsheets, documents, or image files.
- **Remove unauthorized recipients:** When a user accidentally presses "send," make sure you can still scan and inspect the email, to determine if recipients are approved to access it, and then remediate the issue. You should be able to notify the sender of the data found or remove the email recipient altogether before the email is sent.

USE CASE 3

Preventing Accidental Data Shares

Energy Company's HR Data Kept Safe and Accessible in the Cloud

Learn how a large oil organization chose CASB to protect its HR cloud and stay compliant.

READ CASE STUDY ›

It's easy to mistakenly share content through the cloud. Often, this happens by typing in the wrong email address or sharing to someone's personal account instead of their corporate profile. According to the Ponemon Institute, 56% of insider threats are due to this type of negligence. The average remediation cost: $6.6 million.

Precise classification and protection in real time

It's critical that you handle accidental data shares correctly. You can't simply deny access; doing so will cut off collaboration and productivity. Fortra handles such security breaches by providing continuous visibility into data flow and then ensuring that adaptive access can be enforced in real time.

- **Real-time data classification:** Effective protection requires immediate action. As data leaves your SaaS apps, it should be scanned and classified to ensure you can keep track of it.
- **Reversing accidental shares:** If data is erroneously shared with unauthorized individuals, have mechanisms in place that can promptly adjust the sharing settings or entirely remove public shares, so the data breach is confined.
- **Rerouting shares to corporate accounts:** When data is mistakenly routed to personal versions of platforms like Google Workspace, CASB should not only spot the mistake but also ensure the data is redirected to the intended corporate account.
- **Notifications to educate users:** To reduce accidents, your solution should also be able to notify and guide users when they make mistakes.

USE CASE 4

Protecting Data From Malicious Insiders and Account Takeovers

> Thanks to CASB, we can see a surge in downloads from a particular user or timeframe. It turns out none of them presented a threat, but having insight into this activity gave us peace of mind.
>
> **Gary O'Connor, Lantum healthcare organization**

READ CASE STUDY >

Not all threats come from external sources. Sometimes, the most damaging breaches come from existing users that already have access to the organization's infrastructure. Equally dangerous are account takeovers that are a result of social engineering and malware attacks.

Monitor and detect malicious activities

Data exfiltration is tricky to detect because the perpetrators have legitimate access credentials to your organization's cloud resources. To solve this, Fortra's user behavior monitoring and response system uses machine intelligence to identify and convict anomalous behavior.

- **Continuous monitoring of user behavior:** To detect risky or malicious behavior, you need to be able to monitor users in their day-to-day activities, from where they're connecting from, to the apps and devices they use, to how they handle data.
- **Automated policy enforcement:** As soon as any user strays from their normal habits, security protocols and policies should automatically kick in to prevent malicious activities.

USE CASE 5

Safeguard Data From Cloud and SaaS Misconfigurations

How One Fintech Firm Stopped the Leaking From Misconfigurations

Using CASB, a leading fintech organization is able to remediate the leaks that come from their cloud repositories as a result of misconfigurations.

READ CASE STUDY ›

Most organizations now have to juggle dozens of SaaS apps and cloud repositories. While cloud services are more secure in many ways, it's up to you to configure your cloud services properly and protect your data.

Identify and remediate misconfigurations

The problem is, each cloud app has its own settings, so it's nearly impossible to ensure that all of your clouds are properly configured. CASB helps minimize the risk by continuously monitoring your cloud environment to identify gaps between security policies and security posture. This enables you to detect and fix misconfigurations, with remediation options, across cloud environments.

- **Configuration insights across your infrastructure:** To navigate the complexity of numerous services, you need a consolidated look at all your cloud interfaces, giving you unified oversight.
- **Encrypt data with time limits:** Once you assess your configurations, you should ensure they are tuned properly. Your solution should provide recommendations on how to align them with industry standards for security and compliance.

The Power of Fortra's Data-First Approach

Securing access is important to cloud security, but it's not the central challenge. The pivotal concern is identifying the data you possess and ensuring its protection no matter where it goes.

The five use cases described in this e-book are real-world scenarios that our customers in construction, financial services, energy, and healthcare must manage on a regular basis. Situations such as these are why we believe any CASB solution must not only focus on allowing or denying user access to the cloud, but on protecting data even when it's shared via email or through unmanaged apps or devices.

As you contemplate your CASB choice, keep in mind that data protection is paramount and that real-world use cases matter Regardless of what CASB solution you pick, remember that it's a cloud-native DLP you're looking for.

Discover Fortra CASB: A Cloud-Native DLP

With inline and API-based security, Fortra CASB provides visibility and control over users, data, and apps, keeping sensitive data secure and workers productive. Rely on this cloud-native DLP for:workers productive. Rely on this cloud-native DLP for:

- **Real-time visibility into device, user, and data**
- **Centralized policy enforcement across multi-cloud infrastructure**
- **Data protection and accessibility for BYOD, shadow IT, and email**
- **Adaptive zero-trust access**

LEARN MORE ›

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

| fta-cdp-ebook-0625-r1-an