Conquering the Cloud

Data Security and Compliance with a CASB

As organisations migrate to the cloud, they face new data security and compliance risks. A cloud app security broker (CASB) can help mitigate these risks and secure their digital transformation. A CASB can help protect users' accounts, limit access to sensitive data, and unify data loss prevention (DLP) policies across the cloud, email and on-premises file stores.

INTRODUCTION

Migrating your business to the cloud can be a game-changer. It increases your business agility, flexibility and efficiency. But it's also a game-changer when it comes to cybersecurity. Users, apps and data no longer sit behind your network perimeter. Your people share sensitive data without oversight. And cyber criminals can compromise user cloud accounts to steal funds and valuable data. For all their benefits, cloud-based applications and services create new risks and make compliance more challenging. For modern businesses, managing these new risks without squandering the cloud's many benefits can be a delicate balancing act.

COMPLIANCE AND THE CLOUD

Data security and compliance are key parts of that balance.

As your people share and store more of your corporate data in the cloud, your data risks increase. With the adoption of cloud apps, your people can share high-value content through email, link sharing and messaging. This content can include employee or client records, source code, formulas and other confidential documents.

Malicious activity can put your data at risk. So can well-intentioned oversharing of content by your users. That's why you must monitor and govern how your people use data across cloud apps and multiple channels.

Data Security

Half of all reported data breaches result from malicious attacks caused by attackers or criminal insiders. (These include employees, contractors and attackers who misuse insider accounts).[1]

Organisations can be vulnerable because of:

- Weak passwords
- Credential compromise (through phishing campaigns and brute-force attacks)
- A lack of data security measures such as data loss prevention (DLP)

To detect and prevent data breaches in the cloud, you need risk-aware data security. A risk-aware approach connects the dots between compromised accounts and a data breach for better data security.

1 Ponemon Institute. "Cost of a Data Breach Report 2019." July 2019.

Cause and Effect

Once criminals get their hands on user credentials for Microsoft Office 365 or Google G Suite accounts, they use your trusted accounts to launch attacks inside and outside of your organisation.

They solicit fraudulent wire transfers and steal critical data, such as intellectual property or customer data. Or they hijack your email infrastructure to launch internal and external cyber attacks. All of this can have a serious impact on your brand reputation and your bottom line.

Here are just a few examples:

EDUCATION

Cyber criminals see school districts, colleges and universities as "easy prey." These victims have large numbers of students and faculty and decentralised security operations.

The attack: Seventy percent of all educational institutions using cloud services have experienced account takeovers that started with IMAP-based brute-force attacks. Common titles among those targeted include "Professor" and "Alumni."

The aftermath: Attackers use these hijacked accounts to launch spam campaigns or phishing attacks, damaging the institution's brand. The impact of these attacks goes far beyond the targeted entities.

TRAVEL

The attack: The cloud account of the CEO of a major airline was compromised.

The aftermath: Within six days, 40,000 files were downloaded.

REAL ESTATE

According to the FBI, the real estate sector is the most heavily targeted industry for wire fraud.

The attack: Threat actors compromised Office 365 accounts in a 75,000-employee real estate investment firm. Five executives had their accounts taken over.

The aftermath: With access to the executive's email, attackers changed ABA bank routing numbers and siphoned off more than $500,000.

Compliance

When you move data to the cloud, compliance with laws and industry mandates grows more difficult. Compliance mandates are constantly changing. And new rules are stressing data security, privacy and sovereignty.

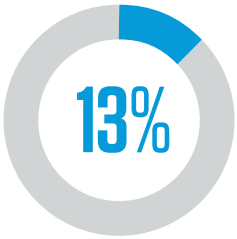
The data types that are of most concern include:

- Customer or employee personally identifiable information (PII) such as Social Security numbers or date of birth
- Consumer payment card information (PCI)
- Protected health information (PHI) such as medical records

Not complying can lead to heavy financial penalties and hurt your reputation and brand. To minimise your compliance risk, you need visibility into your cloud apps. You need to be able to identify and classify data in the cloud. And you need control to prevent unauthorised sharing.

Sharing is Scaring

Among the cloud accounts we've studied:



have broad sharing permissions (external and internal)

are shared with personal accounts that use popular email services

of files in the cloud contain regulated data

Regaining Control

A robust, advanced CASB solution can help you define and apply policies that govern how, when and where your people can access your vital corporate data.

CASB policy parameters should include:

- User roles and risks associated with the login
- Contextual information such as user location and device health

For example, highly regulated sectors such as healthcare have strict policies about accessing sensitive data from unmanaged or risky devices.

To get started, study how data is handled by your cloud apps. Understand your organisation's specific data security goals and use cases for data identification, file remediation, forensics and reporting.

The right CASB solution will allow you to deploy cloud DLP policies consistent with those for email and on-premises file stores. It should also integrate with other DLP solutions to unify incident management.

A CASB WISH LIST FOR DATA DISCOVERY, PROTECTION AND COMPLIANCE

Here's a list of data-protection and compliance capabilities to look for when considering a CASB solution.

Data Discovery

- Discovers sensitive data in both SaaS and Infrastructure-as-a-Service (IaaS) offerings:
  - Microsoft OneDrive
  - Google Drive
  - Box
  - Dropbox
  - AWS S3 buckets
  - Salesforce
  - Mailboxes (Microsoft) Exchange
  - Online Messaging services (Slack and Microsoft Teams)
- Detects sharing permissions for public, external, internal and private files and folders
- Identifies regulated data (PCI, PII, FINRA, HIPAA and GDPR) to assess compliance risks using out-of-the-box and advanced DLP technologies:
  - Identifiers
  - Dictionaries
  - Proximity matching
  - Contextual matching
  - Document fingerprinting
  - Exact data matching (EDM)
  - Optical character recognition (OCR)
- Pinpoints who in your organisation has access to sensitive cloud data

Data Protection

- Seamlessly extends current DLP policies for email and on-premises systems to the cloud
- Quarantines, deletes or removes broad sharing permissions from files with sensitive data
- Sends alerts when sensitive data is being exfiltrated after account compromise
- Automates policy enforcement for file uploads, downloads, collaboration and messaging in the cloud. Uses rules based on the following context:
  - User
  - User group
  - Location
  - Device
  - IP
  - File properties
  - DLP policies
- Alerts security administrators when policy violations occur and notifies users so that they can receive proper coaching

Compliance

- Provides comprehensive audit trails of all file activities. Supports incident investigations with advanced forensics on:
  - File size
  - User
  - DLP matches
  - Sharing permissions
- Integrates cloud DLP incident triage and reporting with those capabilities for other DLP channels, such as email and on-premises data stores
- Integrates with security information and event management and IT service management platforms like ServiceNow to capture alerts for file-handling policies, DLP violations and response actions
- Automates controls for third-party (OAuth) apps to reduce compliance risks

CONCLUSION AND NEXT STEPS

Data security and compliance are key parts of your cloud-first business transformation. To fully defend your organisation in the cloud, you also need to address threat protection and app governance.

A people-centric CASB solution shows you:

- Who in your organisation is most attacked
- Who is vulnerable to attacks
- Who has privileged access to sensitive corporate data

Only this level of visibility and control enables you to keep threats at bay, protect your information assets, and stay compliant.

Download Our Free Guide

Learn more about how a CASB can help you move to the cloud security with our free guide—Getting Started with CASB.

LEARN MORE

For more information, visit **proofpoint.com**.