proofpoint.

E-BOOK

Getting Started with CASB

How Cloud Access Security Brokers Can Help Manage People-Based Risk, Apps and Data in the Cloud

Introduction: Hybrid Work, Digital Transformation and the Cloud

The cloud has been a game-changer for modern business. Cloud platforms and services are key enablers of today's remote, hybrid and mobile workforce. They make business more agile, workplaces more flexible and operations more efficient.

But the cloud is also a game-changer for 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 of a cloud migration can be a delicate balancing act.

Cloud security should start with securing IT-approved applications—such as Microsoft 365 and Google Workspace—that contain your most valuable assets. But most organizations need more visibility into and control over how people access, use and share apps and sensitive data in the cloud.

That's where a cloud access security broker (CASB) solution can help.

What is a CASB solution?

Gartner defines CASB as "products and services that address security gaps in an organization's use of cloud services."[1] While most cloud providers and platforms offer some limited security features, CASBs provide broad visibility into your users, cloud apps and data.

With a CASB, you can extend your corporate security policies to the cloud. You can also get a consolidated view of user and data activity to help and manage and secure it from a single location.

Key capabilities

Today's attacks target people, not technology. That's why an effective CASB solution takes a people-centric approach to securing cloud apps. The right CASB can give you an extra measure of confidence in a cloud-first environment.

Key capabilities should include:

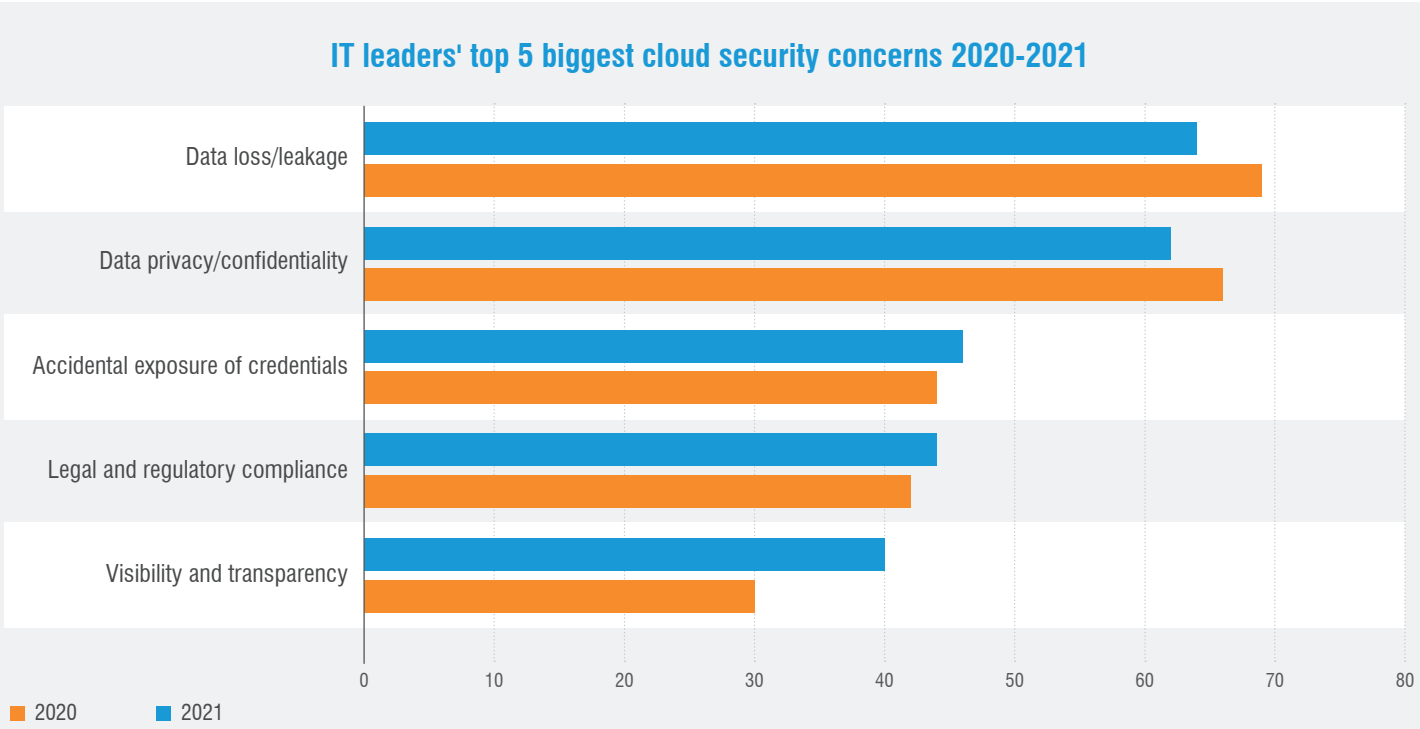
- People-centric visibility to threats and automated response
- Data security, including data loss prevention (DLP), data classification and cloud data discovery
- Cloud and third-party (OAuth) apps governance
- Real-time, adaptive access and data controls for people who pose a higher-than-normal risk
- Infrastructure-as-a-service (IaaS) protection, including cloud security posture management to safeguard against misconfigurations

1 Gartner. "2020 Gartner Magic Quadrant for CASB." October 2020.

Table of Contents

Five Reasons You Need a CASB

More and more enterprises are realizing that a CASB is essential for securing their cloud apps and services. Let's take a deeper look at their biggest concerns.



1. Contain "shadow IT"

Shadow IT refers to the use of cloud apps and services without the explicit approval of IT. Early on, the practice was one of the main drivers of CASB adoption. Users typically use unapproved software-as-a-service (SaaS) applications for file sharing, social media, collaboration and web conferencing.

That behavior persists. But there's another growing challenge: third-party apps and scripts with OAuth permissions. OAuth-connected third-party apps access IT-approved cloud services, such as Microsoft 365 and Google G Suite. Some of these pose risks because of poor design, giving them broader than necessary data permissions.

The danger of OAuth: once a token is authorized, access to enterprise data and applications continues until it's revoked—even if the user's password is changed.

Integrating your CASB solution into your broader web security infrastructure can provide deeper visibility into all unapproved web apps.

CASBs provide visibility into and control over shadow it to limit people-related risk.

2. Protect against cloud threats

Cyber criminals often use compromised cloud accounts to gain access to valuable data and even funds. Once attackers get their hands on cloud account credentials, they impersonate legitimate users. They can trick your people into wiring money to them or releasing corporate data. They can also hijack email accounts to distribute spam and phishing emails.

In a 2021 study of more than 2,800 cloud service tenants with more than 25 million active user accounts, **95%** of tenants were targeted by cyber attacks, and **48%** had at least one compromised account in their environment.

Attackers typically compromise accounts in one of two ways:

- **Brute-force attacks,** a trial-and-error technique where they submit multiple names or passwords to guess the credentials
- **Credential or OAuth token phishing,** where they use socially engineered email to get users to give up their passwords or authorize malicious OAuth apps to access users' data and resources.

CASBs help you detect and respond to unusual account activity, which may indicate compromised credentials. CASBs also help deploy and enforce policies to protect cloud accounts and data.

3. Reduce risk of people-caused data loss and IP theft

Every day, your people use cloud-based collaboration or messaging tools to share files and information with colleagues and partners. At the same time, they can put intellectual property (IP), such as trade secrets, engineering designs and other sensitive corporate data at risk:

Employee negligence or lack of training can result in over-sharing of files via public links, which anyone can access.

Data theft by insiders is also common. For example, salespeople who are leaving your company can steal data from cloud CRM services.

Remote work has also increased the risk of data exfiltration to personal devices. Many employees use unmanaged personal devices to get work done. This means that sensitive data can be stored on devices outside of the control of your IT department.

CASBs can increase visibility into how your people handle data and can improve data security through policies that control access to cloud services based on device, application, user risk and more.

Combining CASB with an enterprise DLP solution offers added security for risk vectors such as email, endpoint, cloud, network file shares and the web. Integrate your CASB with an insider threat management (ITM) solution can offer even stronger protection.

4. Comply with today's evolving regulations

Organizations in nearly every industry are struggling to stay compliant. Many government and industry regulations, like the European Union General Data Protection Regulation (GDPR), require you to know where your data is and how it's shared in the cloud. Violations of data privacy and residency regulations can result in fines of up to 4% of the organization's worldwide annual revenue.

Used with archiving, e-discovery and content supervision solutions, a CASB can reduce cloud and data security headaches at audit time.

5. Avoid cloud misconfigurations that lead to data breaches

Many data breaches are the result of infrastructure-as-a-service (IaaS) and cloud server misconfigurations. That's why understanding the potential risks—and properly configuring your cloud environment—is so critical.

A CASB can alert you to any risks your IaaS configuration poses and help you follow secure configuration best practices for IaaS services such as the Center for Information Security's (CIS) benchmarks for AWS and Azure.

A CASB can help you avoid breaches that stem from cloud misconfigurations.

"The pace of client inquiry indicates that CASB is a popular choice for cloud-using organizations... CASB's growth remains higher than any other information security market."

–Gartner Magic Quadrant for Cloud Access Security Brokers, 2020

Everyone Has a Stake: CASB's Role Across Business Functions

A people-centric CASB solution can address security concerns across key stakeholders in any organization. Here are a few key roles that benefit.

For the CISO, security director, (cloud) security architect, security engineer or security operations manager

You are likely concerned most with:

- Cloud threats that can hurt financials and brand reputation
- Cloud data loss and intellectual property (IP) theft
- Unauthorized access to cloud data and services

Here's how a CASB can help:

- Stop cloud threats before they do damage to company credibility
- Reduce exfiltration of valuable and sensitive information
- Contain "shadow IT"

For the CTO, CIO or director of IT/networking/ infrastructure

You are likely concerned most with:

- Enabling hybrid work to keep users productive in any environment
- Increasing adoption of IT-approved cloud apps through secure access controls
- Simplifying collaboration and data sharing among remote, hybrid and on-site users

Here's how a CASB can help:

- Simplify and secure access to cloud apps through people-centric, adaptive access controls
- Simplify collaboration while protecting sensitive data in the cloud with data-access and sharing controls
- Discover and categorize cloud apps and identify cloud usage

For the chief compliance or risk and privacy officer

You are likely concerned most with complying with today's stricter data protection and privacy regulations.

Here's how a CASB can help:

- Provide "risk-aware" data security and DLP to protect regulated cloud data from unauthorized access
- Minimize compliance risks with comprehensive cloud discovery and governance and automated controls for third-party (OAuth) apps
- Discover IaaS accounts and resources, identify misconfiguration and compliances issues and provide prescriptive guidance for security configurations

Benefits By Industry

Every industry and organization is unique. Here's how a people-centric CASB can benefit yours.

INDUSTRY SEGMENT	TOP CONCERNS	CASB VALUE
 **Financial Services**	Protecting customer financial data from advanced threats, including insider fraud and ransomware, and complying with privacy and data security regulations	Protect customer data and intellectual property through cloud-native DLP and adaptive access controls that integrate zero-trust network access (ZTNA), secure web gateway (SWG) and secure access service edge (SASE) security models with your broader security program.
 **Healthcare**	Patient safety and regulatory compliance	Secure access to patient data and prevent data leakage through adaptive access, unified email and cloud data controls.
 **Government**	Accelerating cloud adoption	Protect from ransomware and insider risks to Microsoft 365 environments through access controls, threat remediation and data loss prevention.
 **Education**	Prevent account compromise and protect student privacy	Safeguard student privacy by controlling access to cloud-based personal information and defend against account compromise.
 **Retail**	Secure cloud adoption and ransomware targeting cloud applications	Protect Microsoft 365 environments containing payment card information through unified and easy-to-setup data and zero-trust access controls.
 **Manufacturing**	Managing access to intellectual property used by third parties in production (such as recipes and CAD drawings) and cyber threats targeting internet of things (IoT) and the cloud	Protect intellectual property, your customers and cloud environments through cloud-native DLP and access controls that are easy for IT teams to set up and maintain.

Cloud account compromise

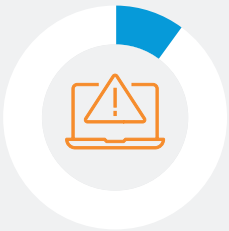
Attackers have a close to 50% chance of getting into a targeted environment via cloud accounts. Just one compromised account can have a big impact on your security.

Among targeted organizations in our research:

95%
of organizations were targeted

32%
of compromised organizations had post-access activity, such as file manipulation, email forwarding, and OAuth app activity

52%
of organizations had at least one compromised account



10%
of organizations had authorized malicious OAuth apps

What Is CASB Good For? Three Use Cases

CASBs can help you address the complexities of cloud security—especially if they take a people-centric approach. They can help you strengthen your security posture by safeguarding your people and your data from advanced threats, prevent data loss and maintain compliance, and control access to SaaS apps.

Let's explore three critical CASB use cases:

1. **Cloud threat protection** (such as such as ransomware, intelligent brute force attacks and advanced phishing campaigns)
2. **Cloud data security and compliance** (such as insider risks and accidental data leakage)
3. **Cloud app governance** (such as such as third-party OAuth applications and shadow IT)

Use case 1:

Cloud threat protection

Today's attacks target people, not technology. This is just as true for the cloud as it is on premises. As businesses move their messaging and collaboration platforms from the corporate network to the cloud, they become vulnerable to attack.

Cyber criminals tend to target popular SaaS applications like Microsoft 365 and Google Workspace. Just about everyone at your company uses these applications, and they hold the key to business communication and vital data. Attackers use a variety of techniques to compromise cloud account credentials and take advantage of vulnerable users.

Geofencing, or blocking network traffic from problem areas, goes only so far. That's because many threats originate from within an organization's own country or region. And geofencing may just not be an option for global companies or those whose workers travel to foreign locations.

A better approach is adaptive access controls such as risk-based authentication, especially if it requires multiple levels of access. Adaptive controls can help you enforce multi-factor authentications during and after login based on security risks, not just on location.

A CASB with a broad complement of security solutions with robust detection, remediation and risk-based authentication capabilities offers the best defense against today's people-centric threats, including brute-force attacks, phishing attacks, malicious file shares and malicious OAuth apps or OAuth abuse.

Intelligent brute-force attacks

Automated tools are used to come up with multiple combinations of usernames with passwords exposed in large credential dumps. These are lists of email addresses, passwords and other information published online after a breach. Attackers can even bypass multi-factor authentication by leveraging legacy email protocols, such as Internet Message Access Protocol (IMAP). This common protocol is used to access email on different devices from the email server and is especially susceptible to cloud attacks.

Ransomware

Ransomware is one of today's most disruptive forms of cyber attack. With just a single username and password—especially for cloud apps such as Microsoft 365 or Google Workplace—a ransomware operator can launch attacks inside and outside of your organization.

CASB controls can be a key defense by:

- Monitoring and detecting compromised cloud accounts
- Monitoring for malicious file uploads to cloud accounts
- Protecting from command and control with web security
- Limiting network access with zero-trust access controls

A modern CASB gives you the visibility to surface the lateral spread or risk to your data because of a compromised account. You can see whether a suspicious login is correlated to an account that sends malicious emails. You'll be alerted if an attacker tried to install persistent access through setting email forwarding and delegation rules or by using OAuth tokens. And can easily learn what suspicious file activity occurred.

Advanced phishing campaigns

These targeted and well-crafted campaigns come in various forms and trick people into revealing their authentication credentials. This gives attackers the opportunity to take over cloud email accounts and impersonate corporate identities.

Research shows that more than 31% of organizations or groups using cloud services experienced account compromise that started with phishing campaigns.[2] To cover their tracks, attackers sometimes leverage virtual private networks (VPNs) or TOR nodes, which preserve a user's privacy and identity. These connection methods can get past certain network access controls used in Office 365, as well as user authentication based solely on location.

Email account compromise (EAC) and business email compromise (BEC) are forms of phishing that target businesses and people who perform wire transfer payments or have access to confidential employee data, such as W-2 tax forms. Cyber criminals typically pose as executives or business partners to prey on victims' trust.

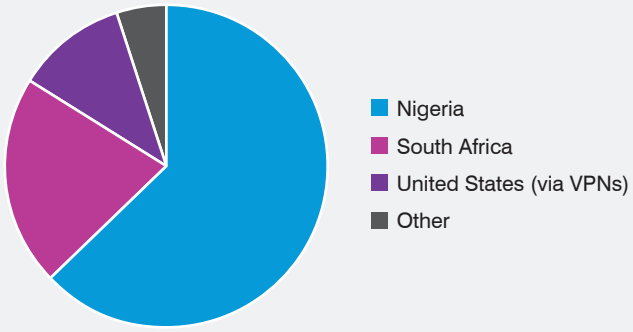
2 Proofpoint research.

Malicious file shares

Phishing links, credential stealers and downloaders are typically used in these types of attacks. Threat actors also distribute malware via cloud services like Dropbox. They leverage these platforms mainly because they are unlikely to be blocked by IT security because nearly everyone uses them. Customer support teams are especially at risk, as they may open malicious files shared by threat actors who impersonate customers.

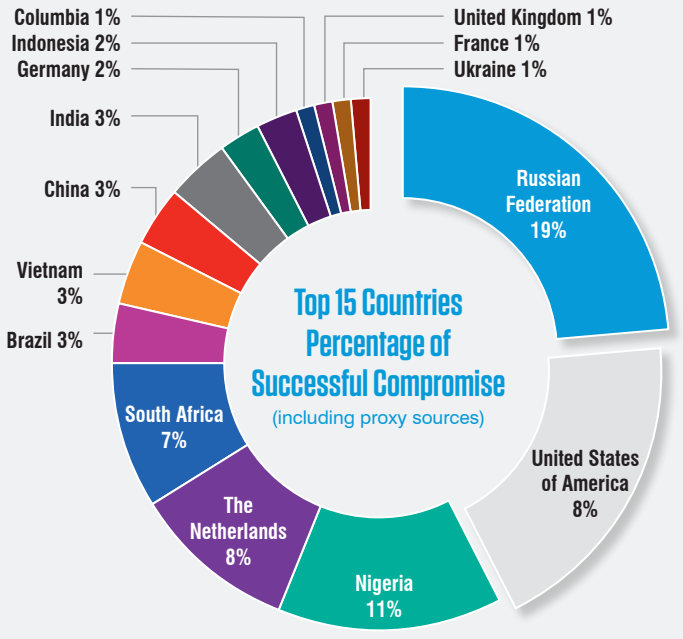
Phishing around the world

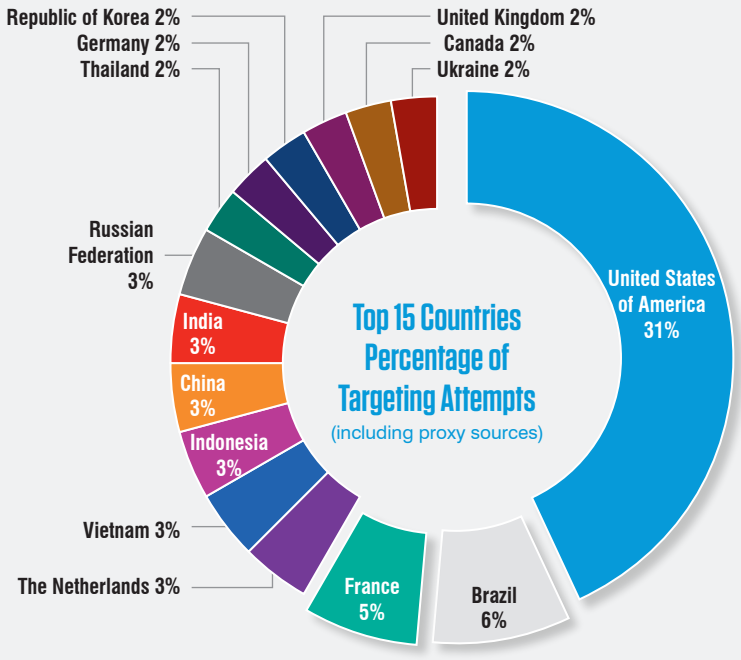
Here's where most phishing campaigns originate:



Source: Proofpoint

Threat landscape – malicious hotspots (January-October 2021)





Source: Proofpoint research

A CASB wish list for cloud threat protection

Here's a list of cloud-threat protection capabilities to look for when considering a CASB solution.

Detection

- Identifies risky users who are highly targeted or have access to critical systems or data
- Provides accurate detection of cloud account compromise through machine learning and threat intelligence
- Correlates email and cloud threats to show how phishing can lead to account compromise
- Identifies suspicious file activity after account compromise, including data exfiltration, upload of malicious files and data destruction
- Tracks down lateral movement of threats after account compromise such as email forwarding and delegation (allows the delegate to read, send and delete messages on the user's behalf) and sending phishing emails
- Captures audit trails of all user activity to aid investigations, complete with advanced forensics on IP address, user agent, location and more

Remediation

- Sends alerts when account compromise or post-compromise activity is detected
- Mitigates risk of account compromise automatically, including support for hybrid Microsoft Active Directory deployments (example actions: terminate session, suspend user accounts or reset password by user or administrator)
- Deletes or quarantines malicious files automatically upon detection
- Includes tools to integrate with and enrich security information and event management (SIEM) threats alert data
- Reverts file sharing permissions and removes malicious files
- Removes delegates and email forwarding rules
- Removes OAuth tokens
- Filters and reports on contextual data, such as users, groups, location, networks, user agent and IP categories, such as TOR, VPN, Proxy and others

Adaptive Access Controls

- Controls access via conditional access rules, such as safelisting and/or blocklisting countries, networks or IP reputation (example: TOR nodes)
- Controls access based on users and groups, such as privileged users with access to critical systems or sensitive data (example: IT administrators), highly targeted persons (example: HR managers) and VIPs (example: board members)
- Prevents risky access based on known threat actor footprints such as IP addresses, user agents and other indicators of compromise
- Enforces step-up authentication policies and limits access levels for off-network devices or based on device health

Use case 2:

Cloud data security and compliance

As your people share and store more of your corporate data in the cloud, the possibility of a breach increases. With the adoption of cloud apps in an era of remote and hybrid work, your people can share high-value content—including sensitive content, like employee or client records, source code, formulas and other confidential documents—through multiple channels: email, link sharing and messaging.

Malicious activity and even well-intentioned oversharing of content by your users can put your data at risk. To prevent data loss and breaches, it's critical to monitor and govern how your people use data across cloud apps and multiple channels.

Data security and insider threats

Half of all reported data breaches result from malicious attacks caused by attackers or criminal insiders (employees, contractors or other third parties). About 19% were due to compromised credentials and another 19% stemmed from cloud misconfigurations.[3]

Weak passwords or credential compromise through phishing campaigns and brute-force attacks, as well as lack of data security measures such as data loss prevention, leave organizations vulnerable to attacks. To detect and prevent data breaches in the cloud, you need risk-aware data security that connects the dots between compromised accounts and a data breach.

Cloud-based file storage apps are common exfiltration points. Our data shows customers are especially concerned about exfiltration to personal cloud storage and USB devices.

But without content awareness, organizations have a hard time knowing whether sensitive data is being moved to personal cloud storage accounts, possibly against policy, or corporate cloud accounts. And without behavior awareness, they can't tell the different between users who are malicious, negligent or compromised.

3 Ponemon. "2020 Cost of a Data Breach Report." June 2020.

SHARING IS SCARING

Among the cloud accounts we've studied:

13%

have broad sharing permissions (external and internal)

5%

are shared with personal accounts that use popular email services

4%

of files in the cloud contain regulated data

Compliance

When you move data to the cloud, compliance with government regulations and industry mandates becomes more difficult than ever before. Compliance requirements are constantly changing, with a growing emphasis on data security, privacy and sovereignty.

The data types that are of most concern are customer or employee personally identifiable information (PII) such as Social Security numbers or date of birth, consumer payment card information (PCI), and protected health information (PHI) such as medical records. Noncompliance can lead to significant financial penalties and potential damage to your reputation and brand.

Getting visibility into your cloud apps, identifying and classifying data in the cloud, and preventing unauthorized sharing are essential to minimize your compliance risk.

Getting back control

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

CASB policy parameters should include user roles, risks associated with the login and contextual information such as user location, device health and others. For example, organizations in 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 and understand your organization's specific data security objectives and use cases for data identification, file remediation, forensics and reporting.

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

Cause and effect

Once criminals get their hands on user credentials for Microsoft 365 or Google Workspace accounts, they leverage your trusted accounts to launch attacks inside and outside of your organization. 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 is most vulnerable

Cyber criminals see school districts, colleges and universities as "easy prey," with large numbers of students and faculty and decentralized security operations.

The attack: Seventy percent of all educational institutions using cloud services have experienced account takeovers that originated from 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, resulting in brand abuse. The impact of these attacks goes far beyond the targeted institutions.

Sensitive data and IP theft

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

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

Wire fraud in real estate

The attack: According to the FBI, the real estate sector is the most heavily targeted industry for wire fraud. Threat actors compromised Microsoft 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.

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 IaaS services:
  - 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 data loss prevention technologies:
  - Identifiers
  - Dictionaries
  - Proximity matching
  - Contextual matching
  - Document fingerprinting
  - Exact data matching (EDM)
  - Optical character recognition (OCR)
- Pinpoints who in your organization has access to sensitive cloud data

Data and insider threat protection

- Alerts security teams when data exfiltration after account compromises, malicious insiders activity and other data security violations occur
- Integrates current DLP policies across email, endpoint, on-premises file shares, cloud and web
- Identifies users sharing sensitive data too widely
- Applies adaptive prevention controls around file sharing and data exfiltration, such as blocking data exfiltration and quarantining, deleting or revoking broad share permissions for sensitive files
- Automates policy enforcement for file uploads, downloads, collaboration, and messaging in the cloud through rules based on context: user, user group, location, device, IP, file properties and DLP policies
- Identifies malicious user activity in the through user behavior analytics
- Integrates with insider threat management and enterprise DLP solutions to protect from malicious and negligent insiders across cloud, email and endpoint

Compliance

- Provides comprehensive audit trails of all file activities and supports incident investigations with advanced forensics on file size, user, DLP matches, sharing permissions and more
- Prevents access to block-listed cloud apps while allowing access to those that meet your security guidelines
- Monitors and limits access to tolerated cloud apps using contextual policies (example: allow only the HR department to access HR applications or limit VAPs access to tolerated apps based on risk)
- Integrates cloud DLP incident triage and reporting with those capabilities for other DLP channels, such as email, endpoint 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 reduce compliance risks

DLP terms

Here's a list of key DLP capabilities for identifying regulated data.

Identifiers: Predefined regular expressions or algorithms that can be used to to identify specific number patterns or character string patterns, which may include mathematical formulas, such as the Luhn algorithm, a modulus 10 algorithm used to identify valid credit card numbers.

Dictionaries, keywords: Collections of words and/or phrases. These are often aligned for a specific regulation or industry such as healthcare, HIPAA, financial, PCI and other related terms.

Proximity matching: A match condition based on how far apart two identifying entities may be. For example, a regular expression and dictionary keyword may have a proximity setting of up to 20 words, which tells the policy to be enforced when the expression and keywords are within 20 words of one another but no more.

Contextual matching: A method of data matching based on factors that don't include the document contents. These external factors may include document header, document size and document format.

Document fingerprinting: Identifies when blocks of texts or forms need to be identified for DLP. Algorithms map documents and files to shorter text strings.

Exact data matching (EDM): A capability that ingests specific database fields and looks for the exact contents of those fields when applying DLP—often used in healthcare to identify documents with specific patient record numbers.

Optical Character Recognition (OCR): The ability to recognize text contained from an image. Often used to identify sensitive information contained within scanned forms or documents.

Use case 3: Cloud app governance

In today's cloud-first world, governing your users' access to both IT-authorized and unauthorized apps (shadow IT) has never been more important. The average enterprise has an estimated 1,000 cloud apps in use. And some of these have serious security gaps that can potentially put organizations at risk and violate compliance regulations and mandates.

An example is users granting broad OAuth permissions to third-party apps. This inadvertently violates data residency regulations, such as GDPR. In addition, attackers often use third-party add-ons and social engineering to trick people into granting broad access to your approved SaaS apps—such as Microsoft 365, Google Workspace and Box—that typically contain sensitive data.

Getting a handle on shadow IT

To get a more accurate understanding of who is using SaaS apps, you need answers to these questions:

- What are the cloud apps used in my organization?
- What are the trends for SaaS adoption and usage? What SaaS apps are overlapping?
- Who is using which application?
- How are these apps being used? Is the use of these applications in accordance with company policy?
- Are these applications risky in terms of security (vulnerabilities and threats) and compliance?
- Which SaaS apps show file upload and download activity?
- Which file uploads and downloads in SaaS apps are violating data loss prevention (DLP) rules?
- Who is uploading or downloading files with DLP violations?

Regulating cloud usage

A CASB solution helps you govern the cloud apps and services your people use by offering a centralized view of your cloud environment. It allows you to get insights into who is accessing what apps and data in the cloud from where and from which device.

CASB catalog cloud services (including third-party OAuth apps) rate the risk level and overall trustworthiness of cloud services and assign them a score. CASBs even provide automated access controls to and from cloud services based on cloud service risk scores and other parameters, such as app category and data permissions.

Malicious OAuth apps and OAuth abuse

An OAuth app is an application that integrates with a cloud service and may be provided by a vendor other than the cloud service provider. These apps add business features and user-interface enhancements to cloud services such as Microsoft 365 and Google Workspace. Enterprise app stores such as Microsoft AppSource and Google Workspace Marketplace offer millions of useful OAuth apps and add-ons: analytics, security, CRM, document management, project management and more.

Most OAuth apps request permission to access and manage user information and data and sign into other cloud apps on the user's behalf. For example, they can access users' files, read their calendars, send emails on their behalf and more.

These add-on apps use OAuth authentication to obtain limited access to cloud services. OAuth enables a user's account information or data to be used by apps without exposing the user's password. OAuth works over HTTPS. It uses access tokens (rather than login credentials) to authorize devices, APIs, servers and applications. OAuth apps can be added to an entire domain or to an individual user account.

Unfortunately, OAuth apps can easily be exploited. Attackers can use OAuth access to compromise and take over cloud accounts. Until the token is explicitly revoked, the attacker has persistent access to the user's account and data.

Given the broad permissions they can have to your core cloud applications, OAuth apps have become a growing attack surface and vector. Attackers use various methods to abuse OAuth apps, including compromising app certificates, which was also used in the SolarWinds/Solorigate campaign.

A CASB wish list for cloud app governance

Here's a list of cloud-app governance capabilities to look for when considering a CASB solution.

Visibility

- Discovers cloud services in use and catalogs them by:
  - Ingesting network traffic logs automatically from firewalls, and secure web gateways such as Zscaler, Palo Alto Networks, Checkpoint and others
  - Detecting and assessing OAuth permissions for third-party apps that access cloud apps like Microsoft 365 and Google Workspace
  - Discovering and surfacing IaaS accounts, resources and misconfigurations
- Detects the number of users and data traffic for cloud services
- Identifies who in your organization is accessing which cloud services
- Categorizes each cloud application and service (example: financial, games, human resources and other)
- Assesses cloud service security risks and compliance gaps and assigns a risk score to each service
- Identifies files uploads and downloads and the user involved

Controls

- Provides alerting and coaching capabilities for end users
- Provides compliance reporting capabilities
- Applies cloud governance policies and automates controls for cloud access such as "allow," "read-only" or "block" based on app risk score and app category
- Revokes OAuth permissions for third-party apps based on severity of risk, app scope, category and other characteristics, such as user/groups
- Controls file uploads to and downloads from unapproved cloud applications by leveraging web isolation and DLP technologies to protect users from threats and data loss

Proofpoint Integrations

- Gets visibility and control over shadow IT and web apps with security service edge (SSE) integrations, including:
  - Proofpoint Web Security
  - Proofpoint Browser Isolation
  - Proofpoint Zero Trust Network Access
- Offers added data protection by integrating with:
  - Proofpoint Enterprise DLP
  - Proofpoint Insider Threat Management

Contending with the cloud

The 2019 Cloud Security Report indicates that the top operational security headaches that security operations center (SOC) teams are struggling with are:

Compliance (34% of those surveyed)

Before adopting cloud apps or allowing their use, IT teams need to make sure these apps support compliance with privacy regulations such as GDPR, PCI-DSS, HIPAA and others.

Lack of visibility (33% of those surveyed)

Visibility doesn't just address security and compliance gaps. It also offers the ability to eliminate redundancies, adopt cloud apps that are becoming popular, and roll these apps out to other parts of the organization.

(Source: Cybersecurity Insiders)

CASB Deployment Modes

CASBs can be deployed in a number of configurations, but each approach has benefits and downsides.

Forward proxy

In this “first-mile” inline deployment, the CASB intercepts user traffic to govern application access and apply data controls. It can route traffic using any one of a number of techniques, such as DNS redirect, firewall-enabled forwarding, proxy auto-configuration (PAC) files or endpoint agents.

Reverse proxy

As “last-mile” inline deployment, a reverse proxy deployment puts the CASB in front of the cloud service. After they’ve been authenticated though an identity-as-a-service (IDaaS) provider, users are directed to the CASB, which in turn manages access to the cloud application. Reverse-proxy deployments can apply controls such as step-up authentication.

API mode

In this deployment, the CASB uses out-of-band application programming interfaces (APIs) to receive and analyze cloud traffic data such as log events, data files, user activity and more. The CASB enforces security policy and remediates access issues with features such as:

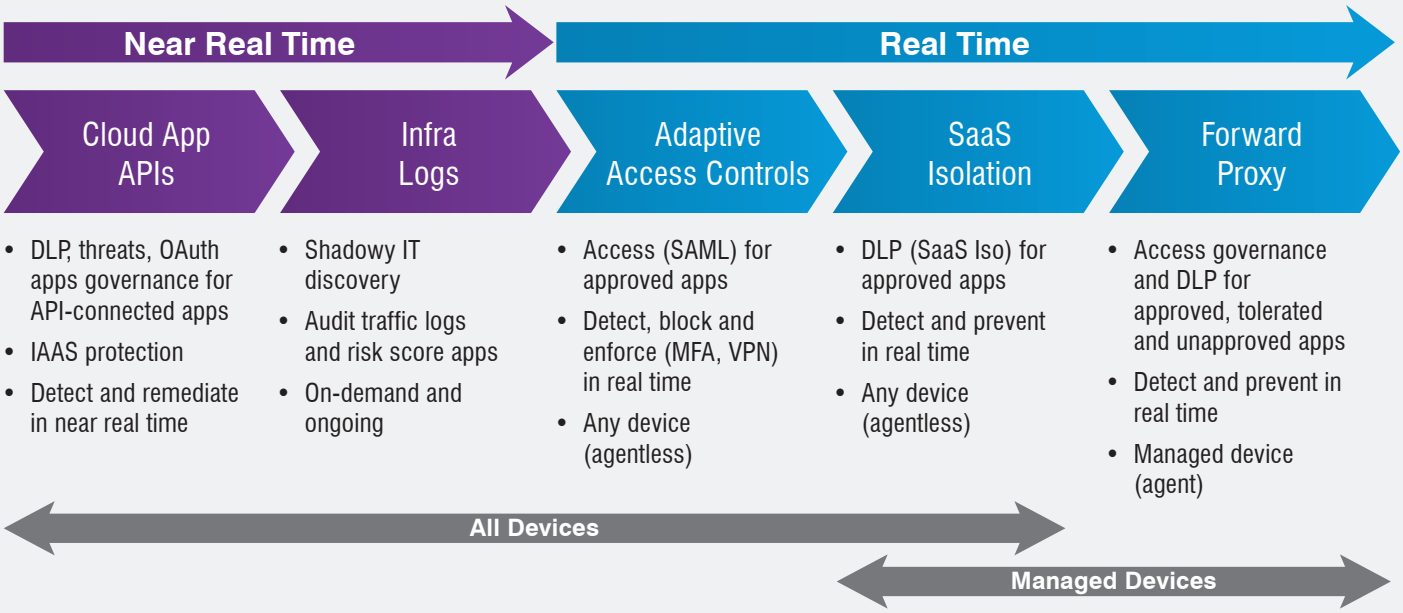
- Revoking user sessions
- Revoking OAuth tokens
- Suspending user accounts
- Forcing users to change their password
- Reducing file-sharing permissions

Adaptive access controls

Adaptive access controls are an alternative to reverse proxy. They use Security Assertion Markup Language proxy and web isolation technologies to apply risk-based controls as needed. The best CASBs can apply these controls to users who pose a higher-than-normal risk to the organization, such as:

- High-privilege users
- Users targeted by an usually high volume or highly sophisticated attacks
- Users shown to be especially susceptible or vulnerable to phishing tactics

CASB Multi-mode architecture



Conclusion: Next Steps

Security is a key part of your cloud-first business transformation. To fully defend your organization in the cloud, you need to address threat protection, data security, and app governance. A people-centric CASB solution accounts for who is most attacked, who is vulnerable to attacks, and who has privileged access to sensitive corporate data.

This level of visibility and control enables you to keep threats at bay, protect your information assets and stay compliant. Proofpoint provides the only CASB to meet the needs of security people serious about cloud threats, data loss and time-to-value. Proofpoint CASB is built on an agentless cloud security architecture. It protects your most valuable cloud assets and accelerates your migration to the cloud.

Proofpoint Cloud App Security Broker

For security people serious about cloud threats, data loss and time to value, Proofpoint CASB provides a full range of capabilities. With Proofpoint CASB, you can:

- Extend people-centric threat visibility and adaptive controls to cloud apps
- Deploy cloud DLP policies consistent with those for email and on-premises file repositories and centralize DLP incident management across cloud apps and other Proofpoint DLP solutions on the CASB console
- Discover cloud apps and contain shadow IT, including third-party OAuth apps that access Microsoft 365 and Google Workspace data
- Respond and remediate faster through the integration with Proofpoint TAP and TRAP
- Implement enterprise-wide information protection with Proofpoint Information Protection
- Integrate visibility, detection and remediation telemetry into SIEMs through our restful APIs and data-export features
- Expand cloud security use cases with Proofpoint Web Security, Proofpoint Zero Trust Network Access and Proofpoint Cloud App Security Broker
- Deploy and enforce people-centric security policies with Proofpoint Nexus People Risk Explorer

Cloud App Security Broker

Threat Protection	Data Security	App Governance
		
• Detect and remediate account takeover • Adaptive controls, including multifactor authentication (MFA),, to protect from unauthorized access to IT-approved cloud apps • Advanced malware protection powered by Proofpoint TAP	• Discover sensitive data • Monitor risky, excessive data sharing • DLP unified across email, endpoint, on-premises file shares and web channels	• Identify and audit cloud app usage (including shadow IT) • Detect and mitigate malicious third-party (OAuth) apps • Cloud security posture management

Learn More

Find out how we can help you move forward more confidently with your cloud strategy at **proofpoint.com/us/products/cloud-security/cloud-app-security-broker**

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.