EBOOK

Getting Started with CASB

Gaining Visibility and Protection for Your People, Apps and Data In The Cloud

proofpoint.com

The promise and peril of the cloud

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 creates new risks and makes 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 Office 365 and Google G Suite—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 cloud providers offer limited security, CASBs provide broad visibility into your users, your cloud apps, and your data.

With a CASB, you can extend your corporate security policies to the cloud and better secure cloud services.

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)
- Cloud and third-party (OAuth) apps governance
- Adaptive access controls for additional layers of security for people who pose a higher-than-normal risk

CONTENTS

2 The promise and peril of the cloud

3 Four reasons you need a CASB

5 Three CASB use cases

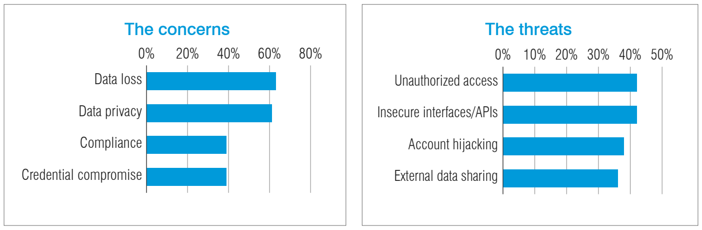
10 Conclusion: Next steps

[1] Gartner. "Magic Quadrant for Cloud Access Security Brokers." October 2018.

Four 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.

Top cloud security issues



(Source: Cybersecurity Insiders)

1. Contain "shadow IT"

Shadow IT refers to the use of cloud apps and services without 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 Office 365 and Google G Suite. Some of these pose risks because of poor design, giving them broader than necessary data permissions.

What's the danger of OAuth? Once an OAuth token is authorized, access to enterprise data and applications continues until it's revoked.

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 study of more than 1,000 cloud service tenants with more than 20 million user accounts, more than 15 million unauthorized login attempts took place in the first half of 2019 alone. More than 400,000 of these attempts resulted in successful logins. In all, about **85%** of tenants were targeted by cyber attacks, and **45%** had at least one compromised account in their environment.[2]

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 phishing, where they use socially engineered email to get users to give up their passwords

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

3. Reduce risk of 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.

CASBs can increase visibility into how your people handle data and can improve data security through policies that control access to cloud services.

4. Compliance with today's stricter 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.

CASBs can ease the compliance burden and spare you headaches at audit time.

> "... by 2022, 60% of large enterprises will use a CASB to govern some cloud services, up from less than 20% today."
>
> —Gartner Magic Quadrant for Cloud Access Security Brokers, 2018

[2] Gartner. "Magic Quadrant for Cloud Access Security Brokers." October 2018.

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.

CISO, Security Director, (Cloud) Security Architect, Security Engineer

These roles are concerned with the following issues:

- 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"

CTO, CIO, Director of IT/Networking/ Infrastructure

These roles are concerned with the following issues:

- Safe adoption of IT-approved cloud apps while keeping users productive
- Controlling access to IT-approved cloud apps without sacrificing user productivity
- Secure sharing of cloud data

Here's how a CASB can help:

- Address the risk of cloud apps without impacting productivity through people-centric adaptive controls
- Secure cloud data without interfering with collaboration
- Discover and categorize cloud apps and identify cloud usage

Chief Compliance or Risk and Privacy Officer, SOC Manager

These roles are concerned with complying with today's stricter data protection and privacy regulations.

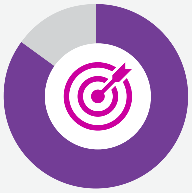
Here's how a CASB can help:

- 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

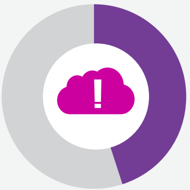
Cloud account compromise

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.

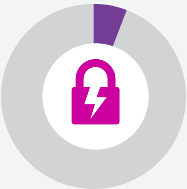
Among targeted organizations in our research:



85% were targeted at least once by attackers



45% had at least one cloud account compromised



6% had a VIP account compromised

13 active accounts on average experienced unauthorized logins

(Source: Proofpoint)

Industry focus

Here's how a people-centric CASB solution solves industries' top concerns.

Industry Segment	Top Concern	**CASB Value:** Secures Office 365 and other IT-approved cloud apps to protect…
Financial Services	Compliance with today's stricter data protection and privacy regulations	Customer privacy by controlling access to cloud-based financial information
Healthcare	Patient safety and regulatory compliance	Patients and their data by controlling access to cloud-based health information
Government	Accelerating cloud adoption	Employee and citizen privacy by controlling access to cloud-based sensitive information
Education	Prevent account compromise and protect student privacy	Student privacy by controlling access to cloud-based personal information and defend against account compromise
Retail	Innovation and faster cloud adoption	Customer privacy by controlling access to cloud-based personal and payment card information
Manufacturing	Innovation and faster cloud adoption	Customer privacy and IP by controlling access to customer and IoT project information

Three CASB 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
2. Cloud data security and compliance
3. Cloud app governance

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 Office 365 and Google G Suite. 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 and malicious file shares.

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.

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.[3] 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.

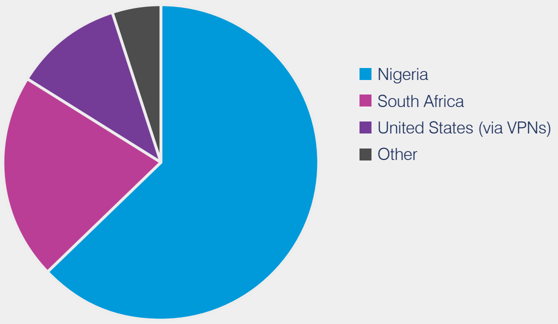
Email account compromise (EAC) and business email compromise (BEC) are forms of phishing that target businesses and people who perform wire transfer payments or have access to confidential employee data, such as W-2 tax forms. Cyber criminals typically pose as executives or business partners to prey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

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 compaigns originate:



(Source: Proofpoint)

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 attempts to access data after account compromise
- 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)
- 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 SIEM threats alert data
- Reverts file sharing permissions
- 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

Risk-based authentication

- 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 stepped-up authentication policies and limits access levels for off-network devices or based on device health

[3] Proofpoint. "Cloud Attacks Prove Effective Across Industries in the First Half of 2019." September 2019

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, 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

Half of all reported data breaches result from malicious attacks caused by attackers or criminal insiders (employees, contractors or other third parties).[4]

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.

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.

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

(Source: Proofpoint)

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 like 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 data loss prevention (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 Office 365 or G Suite 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 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.

[4] Ponemon Institute. "Cost of a Data Breach Report 2019." July 2019.

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) 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 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 through rules based on context: user, user group, location, device, IP, file properties and 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 and supports incident investigations with advanced forensics on file size, user, DLP matches, sharing permissions and more
- 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 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: A condition that determines 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: Includes external factors such as header, size, format, and others—anything that doesn't include the content of the document.

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 Office 365, G Suite and Box—that typically contain sensitive data.

Getting answers

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.

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 Office 365 and G Suite
- 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

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)

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-based IT, including third-party OAuth apps that access Office 365 and G Suite data

Threat protection

- Compromised accounts detection and remediation
- Malware protection

Data security

- Unified DLP across channels
- Built-in data classification

Cloud governance

- Shadow IT visibility
- OAuth-based third-party apps protection

Access control

- Risk-based authentication
- Adaptive access controls
- Security orchestration

Cloud services integrations

Dropbox · Office · slack · amazon web services™ · box

G Suite · okta · salesforce

FIND OUT HOW

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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**.