proofpoint.

SOLUTION BRIEF

Proofpoint CASB Real-Time Controls for Approved and Tolerated Apps

People-centric data and access controls for cloud apps accessed from managed devices

Challenges

- Sensitive data loss and compliance
- Use of unapproved cloud apps
- Lack of visibility and data controls for remote workers

Key Capabilities

- Real-time data controls for all cloud apps
- Access governance for unapproved apps

Products

- Proofpoint Cloud App Security Broker Proxy (CASB Proxy)
- Proofpoint SaaS Isolation

Why Proofpoint?

- People-centric data security controls (Very Attacked People™, privileged users and users vulnerable to cyber attacks)
- Common DLP classification across email, cloud apps and endpoint
- Sophisticated analytics in a unified Information Protection Platform

As more people work remotely, the network perimeter is replaced by a people perimeter. Safe data handling on endpoints and cloud apps has become a priority. To protect enterprise data and ensure compliance, you need visibility into risky behavior by remote workers such as:

- Downloading sensitive data from IT-approved applications
- Sharing confidential data using third-party file sharing sites
- Storing enterprise data on personal cloud storage
- Using unapproved cloud applications, such as chat and conference apps

Controlling file sharing in the cloud and governing access to unapproved apps require real-time data loss prevention (DLP). CASB Proxy identifies and classifies regulated data such as PHI, PCI and PII. It monitors sensitive data as they are being uploaded, downloaded or shared in the cloud. In addition to regulated data, it monitors intellectual property and confidential documents such as:

- Source code
- Design documents
- Legal documents
- Engineering documents

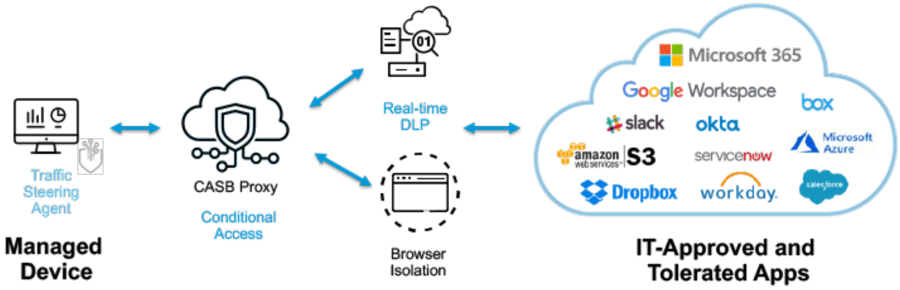


Figure 1: How Proofpoint CASB Proxy protects your cloud apps.

CASB Proxy detects metadata tags and labels, such as confidential, highly confidential and other sensitivity labels. By using our proxy's contextual and people-centric policies, you can apply real-time granular data controls over cloud activity. In doing so you prevent data loss and compliance violations.

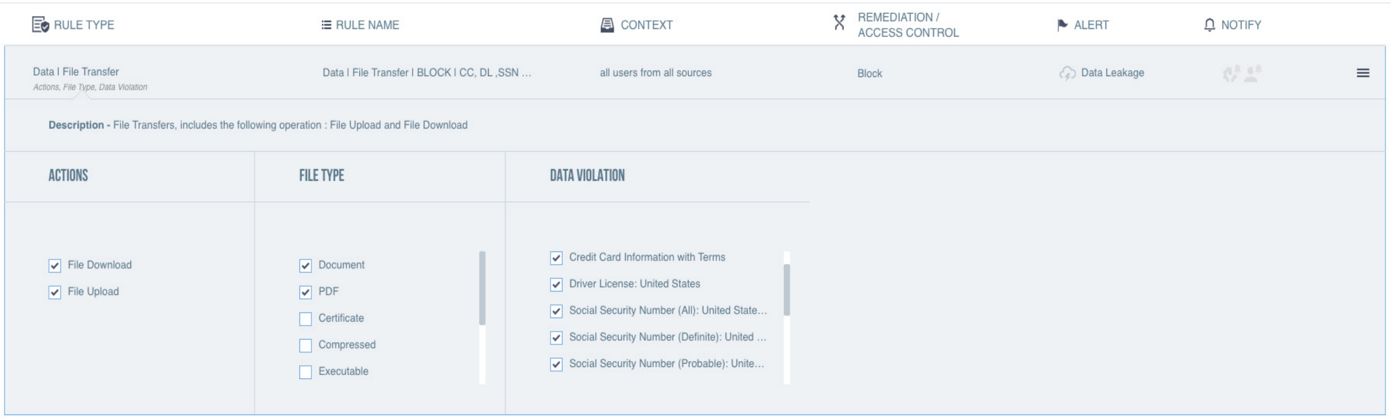
With the help of a lightweight endpoint agent, our cloud-hosted solution provides data controls for approved and tolerated applications.

CASB Proxy is an integral part of our Information Protection platform. Proofpoint Information Protection is a new people-centric approach to protecting against data loss across email, cloud apps and endpoint. Our platform bridges across all DLP channels using a common data classification framework. It combines content-, behavior- and threat-based telemetry with sophisticated analytics. And it addresses the full spectrum of data loss scenarios of malicious, negligent and compromise users. Our unified alerts and investigations interface lets your security and compliance teams to:

- Prioritize alerts efficiently
- Respond faster
- Achieve a shorter time to value

People and data-centric controls for real-time DLP

With CASB Proxy, you can apply people-centric policies when users are uploading and downloading sensitive files and sharing them across approved and unapproved cloud apps. You can enforce stricter data controls for those risky



RULE TYPE	RULE NAME	CONTEXT	REMEDIATION / ACCESS CONTROL	ALERT	NOTIFY
Data I File Transfer *Actions, File Type, Data Violation*	Data I File Transfer I BLOCK I CC, DL ,SSN ...	all users from all sources	Block	Data Leakage	

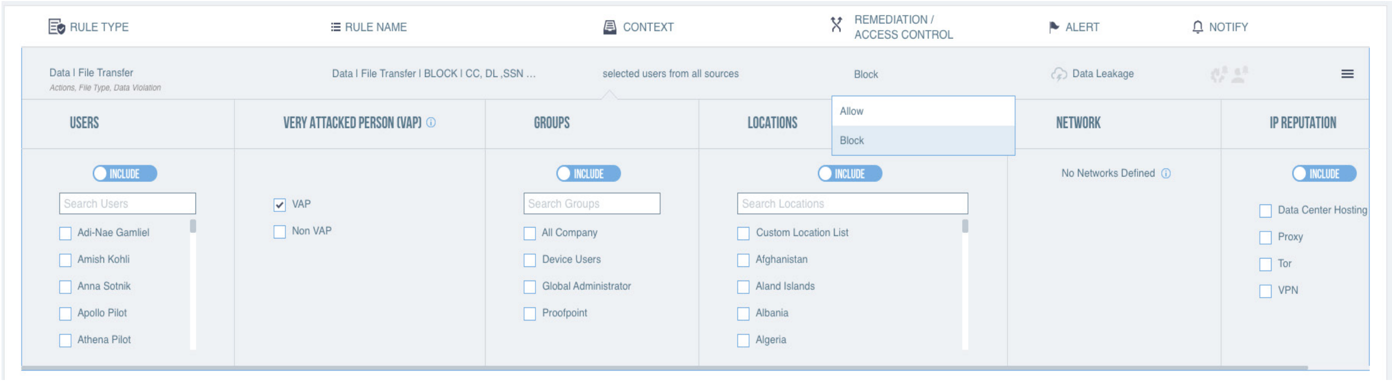
Description - File Transfers, includes the following operation : File Upload and File Download

ACTIONS
- ☑ File Download
- ☑ File Upload

FILE TYPE
- ☑ Document
- ☑ PDF
- □ Certificate
- □ Compressed
- □ Executable

DATA VIOLATION
- ☑ Credit Card Information with Terms
- ☑ Driver License: United States
- ☑ Social Security Number (All): United State…
- ☑ Social Security Number (Definite): United …
- ☑ Social Security Number (Probable): Unite…

Figure 2a: File upload and download DLP rule for VAP—content specifications.



RULE TYPE	RULE NAME	CONTEXT	REMEDIATION / ACCESS CONTROL	ALERT	NOTIFY
Data I File Transfer *Actions, File Type, Data Violation*	Data I File Transfer I BLOCK I CC, DL ,SSN ...	selected users from all sources	Block Allow Block	Data Leakage	

USERS
INCLUDE
Search Users
- □ Adi-Nae Gamliel
- □ Amish Kohli
- □ Anna Sotnik
- □ Apollo Pilot
- □ Athena Pilot

VERY ATTACKED PERSON (VAP)
- ☑ VAP
- □ Non VAP

GROUPS
INCLUDE
Search Groups
- □ All Company
- □ Device Users
- □ Global Administrator
- □ Proofpoint

LOCATIONS
INCLUDE
Search Locations
- □ Custom Location List
- □ Afghanistan
- □ Aland Islands
- □ Albania
- □ Algeria

NETWORK
No Networks Defined

IP REPUTATION
INCLUDE
- □ Data Center Hosting
- □ Proxy
- □ Tor
- □ VPN

Figure 2b: File upload and download DLP rule for VAP—user, location, IP reputation and other contextual specifications.

users or privileged groups such as admins. Risky users maybe negligent, malicious or Very Attacked People (VAPs). VAPs are highly targeted by attackers. They have unique professional contacts and privileged access to data, systems and resources. Or they are prone to clicking unsafe links or using untrusted networks.

CASB Proxy also provides data-centric controls. For those tolerated cloud apps, you can monitor file sharing activity and block sensitive content uploads. You can also limit uploads of certain type of data to specific applications.

CASB Proxy addresses and coaches users on the following people- and data-centric DLP use cases:

- Limit upload and download of sensitive content for VAPs
- Prevent malicious users from exfiltrating confidential documents from IT-approved cloud apps or uploading them to unapproved cloud storage.
- Block unauthorized users from downloading regulated data from IT-approved applications. For example, block an HR partner in US from downloading EU PII data.
- Prevent negligent users from uploading sensitive content from managed device to tolerated cloud apps.
- Stop negligent user from uploading confidential files from managed device to personal instance of a IT-approved application.
- Isolate personal versions of cloud storage and restrict access to read-only.
- Allow upload of PCI data to specific applications only

Cloud application access governance

CASB gives you visibility into cloud usage across your organization. We help you audit network traffic logs and discover cloud apps and who uses them. Our catalog has 46,000 applications with more than 50 risk attributes per app. The cloud apps are categorized by type and risk score. Using our application catalog, you can determine security risks, data loss vulnerabilities and non-compliance. You can govern access to IT-approved and unapproved applications.

We address the following access governance use cases:

- Prevent access to block-listed cloud apps while allowing access to those that meet your security guidelines
- Monitor and limit access to tolerated cloud apps using contextual policies (e.g., allow only the HR department to access HR applications or limit VAPs access to tolerated apps based on risk).

Deploy quickly in the cloud

Our endpoint agent directs your cloud app traffic to our cloud-hosted proxy. The CASB proxy governs access to IT-approved and unapproved cloud applications. For business applications, CASB proxy applies data controls based on DLP policies. For risky cloud apps, we redirect traffic to Proofpoint SaaS Isolation to prevent data theft or loss while providing the user read-only access.

Compared to other proxy-based approaches, our solution offers distinct architectural advantages for real-time access governance and DLP. Here are a few:

- Works with managed devices. You can govern access to cloud apps and prevent data loss for any user on and off the corporate network for corporate-managed devices.
- Works with any app. The CASB proxy can support any cloud app, IT-approved or unapproved.
- Lightweight endpoint agent. Our endpoint agent for split tunneling requires minimal CPU resources.
- Interoperable with third parties: Our endpoint agent is compatible with Proofpoint and third-party secure web gateways.
- Robust and scalable. The CASB proxy is globally deployed on public cloud. Granular admin controls enable you to disable traffic steering based on users/groups, location and more in case of performance issues such as latency in certain locations.
- Offers user privacy. Unlike other inline solutions, the proxy neither inspects all data nor does it have visibility to user credentials. If the user is redirected to browser isolation for data loss prevention, only file transfers are inspected. And no data is stored unless there is a policy violation. This preserves the user's and organization's data privacy.

Products

Proofpoint CASB Proxy

CASB Proxy is a forward proxy that provides real-time control from managed devices accessing the cloud. Our proxy analyzes cloud traffic in real time to classify content and enforce DLP and access governance policies. Our proxy is an optional add-on to Proofpoint CASB. CASB combines compromised account detection, data loss prevention (DLP), cloud and third-party apps governance with people-centric controls. It helps you secure Microsoft 365, Google Workspace, Box, Salesforce, Slack and more.

Proofpoint SaaS Isolation

SaaS Isolation is an optional add-on to CASB. It secures users' access to cloud apps and data by isolating browser sessions in a secure container. This unique solution secures file uploads and downloads for risky users and behaviors. And it applies cloud DLP policies to file transfers in real time, preventing theft or loss of sensitive data. Also, it helps you solve the security, productivity and privacy challenges that come with high-risk cloud use. SaaS Isolation supports all cloud applications through integration with our CASB proxy solution for managed devices. SaaS Isolation also supports any IT-approved application through our agentless architecture for unmanaged devices. It's simple to deploy, manage and support.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) 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.

proofpoint.