Proofpoint Cloud App Security Broker

Secure your cloud users, apps and data from threats, data loss and compliance risks

Key Benefits

- Provide visibility into cloud threats, risky data movement in the cloud and risky cloud app usage
- Defend against data loss by integrating cloud with email, endpoint and web DLP in the Information and Cloud Security platform
- Discover regulated and sensitive cloud data
- Protect cloud users and cloud accounts from account takeovers, OAuth app abuse, persistent access and malicious files
- Govern cloud usage with discovery and dynamic risk assessment, including third-party OAuth apps
- Deploy CASB through API connectors, adaptive access controls and a forward proxy to optimize your time to value and real-time control needs

Proofpoint Cloud App Security Broker (CASB) extends data loss prevention (DLP) and threat protection from email to cloud apps. It combines people-centric threat protection, data security (including inline DLP) and cloud app governance.

Proofpoint CASB allows you to see who creates sensitive data. It also lets you see who owns, downloads, uploads, shares and edits that data. With it, you can protect files in your cloud apps that violate DLP rules from negligent or malicious data loss. And our analytics and adaptive controls help you grant the right levels of access to users and third-party OAuth apps. We base these levels on the dynamic risk factors across behaviors and threats that matter to you.

Extend Proofpoint Threat Protection From Email to Cloud Apps

Proofpoint CASB helps protect the cloud accounts of your people, including Very Attacked People™ (VAPs), executives and suppliers. It protects users from cloud threats such as malicious files, account takeovers, unauthorized access and risky misconfigurations. We leverage the world-class threat intelligence of Proofpoint Targeted Attack Protection (TAP) and Emerging Threats (ET) Intelligence. You can extend security controls with Proofpoint Threat Response Auto-Pull (TRAP) and Security Awareness Training (PSAT) for cloud apps. Proofpoint CASB also leverages the visibility of Proofpoint TAP, Browser Isolation and Web Security for shadow IT discovery.

Unify DLP Across Cloud, Email, Endpoint and Web

Proofpoint CASB is an integral component of the Information and Cloud Security platform. This platform consolidates cloud data loss events and alerts from CASB with the rest of Proofpoint Enterprise DLP in timeline-based workflows. You have visibility as users move sensitive data in and out of cloud apps from other channels such as endpoints, email and websites.

You can use DLP classifiers across channels. More than 240 built-in classifiers cover PCI, PII, PHI and GDPR. Custom contextual rules and advanced detection, such as exact data matching, also let you build your own DLP policies. You can also add optical character recognition (OCR) to your detectors. This lets you identify sensitive data in images. All these can help you protect sensitive data in SaaS apps, IaaS buckets, email, endpoint and web channels.

Proofpoint CASB Proxy and Proofpoint Browser Isolation feature inline controls. These let you restrict data exfiltration from unmanaged devices. They also help prevent sensitive file uploads to unapproved cloud apps in real time. With API connectors, you can reduce sharing permissions for files and IaaS buckets. You can also correlate suspicious logins or misconfigured AWS S3 buckets with DLP incidents.

Protect Users From Cloud Threats

Proofpoint CASB correlates user identities with cloud, email, web and third-party threat intelligence. This helps you know when a cloud account has been compromised. You can also spot user enumeration brute-force attacks and risky configurations that are used for suspicious activity and that can enable cloud ransomware.

Proofpoint CASB automatically correlates cloud attacks in your environment from initial access to post-access suspicious email, data and third-party OAuth app activity. With timeline-based views, it gives you the threat behavior and data context you need to respond to sophisticated cloud threats. Our remediation policies are based on your needs and standards. They let you suspend compromised accounts, for example. You can also quarantine malicious files and revoke malicious OAuth apps. With adaptive access controls, you can integrate your identity management solutions through SAML authentication. Risk-based SAML authentication and isolation help prevent unauthorized access to corporate apps and secure your remote workers.

Govern Cloud and Third-Party Apps

Proofpoint CASB simplifies cloud governance and compliance. It helps you reduce your cloud and web app attack surface. It features app discovery as well as dynamic prioritization of cloud and web apps. Proofpoint CASB also provides dynamic intelligence around sensitive data, user privileges and user behavior patterns.

Our risk model integrates vulnerability, attacks and privilege associated with each app. Compensating controls within the platform let you block risky apps and grant users read-only access to them. You can step up authentication when users access high-risk apps. You can also revoke access to malicious third-party apps.

We discover cloud apps using Proofpoint Browser Isolation, Secure Access, TAP, Web Security and your network firewall logs. Our catalog has 43,000 apps with more than 50 app attributes. We assess OAuth permissions for third-party apps and scripts that access your IT-approved cloud services. You can also discover approved and unapproved IaaS accounts and resources.

Deploy Quickly With a Multimode Architecture

Our multimode CASB architecture helps you secure your cloud apps and services with speed and flexibility. You can start with cloud API connectors to your critical IT approved apps. You can then add adaptive access controls and SaaS isolation for unmanaged devices. You can also deploy CASB Proxy to govern approved and unapproved apps on managed devices.

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 75 percent 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**.