Proofpoint Cloud App Security Broker

Gain visibility and control of your cloud apps

**KEY BENEFITS**

- Discover cloud use, assess risk of cloud apps and contain shadow IT, including third-party OAuth apps
- Protect cloud users with people-centric threat visibility and response
- Govern cloud use with real-time controls for users on-premises and remote regardless of device type
- Shorten time to discover and protect regulated cloud data with out-of-the-box DLP
- Protect sensitive data with accurate DLP that combines content, behavior and threat telemetry
- Simplify DLP operations with a unified alert manager across cloud, email, web and endpoint (in our Information and Cloud Security Platform)
- Identify IaaS accounts and resources, monitor accounts for suspicious activity and manage cloud security posture
- Install in days and achieve actionable results in less than four weeks

Proofpoint Cloud App Security Broker (CASB) takes a people-centric approach to protect your users from cloud threats and safeguard your sensitive data. It also helps you discover shadow IT and govern the use of cloud and third-party OAuth apps.

Cloud security starts with safeguarding IT-approved apps that contain your most valuable data. These apps include Microsoft 365, Google Workspace (formerly G Suite), Salesforce, Box and others. Our integrated, people-centric approach correlates threats and applies consistent data loss prevention (DLP) policies across cloud apps, email, web and endpoint (as part of the Proofpoint Information and Cloud Security Platform).

Proofpoint CASB protects you from account compromise, malicious files and OAuth abuse. It also protects you against unauthorized access, oversharing of data, misconfiguration of IaaS resources and compliance risks. Our multimode architecture gives you people-centric visibility into threats, inline access and data controls, automated responses and comprehensive data security with DLP. It helps you govern SaaS and third-party OAuth apps as well as IaaS services for a strong cloud security posture.

**Extend People-Centric Visibility to Cloud Apps**

Proofpoint CASB provides you with people-centric visibility into email and cloud threats. We help you identify your Very Attacked People™ (VAPs). And we protect their cloud accounts and data. You can see the files in your cloud apps that violate DLP rules. You can also see who owns them as well as who downloads, shares and edits them. And our analytics and adaptive controls help you grant the right levels of access to users and third-party OAuth apps based on the risk factors that matter to you.
Protect Users From Cloud Threats

Proofpoint CASB combines user-specific contextual data with rich cross-vector (cloud, email and more) threat intelligence from Proofpoint Nexus Threat Graph. We use machine learning and threat correlation. This helps you detect when a cloud account has been compromised and is being used for suspicious activity. Such activity may include sending or forwarding emails and exfiltrating data.

The Proofpoint CASB dashboard is intuitive. It lets you easily investigate alerts for suspicious logins as well as file and administrative activity. You can export forensics data to a security information and event management (SIEM) solution for further analysis. You can do this manually or with REST APIs.

We protect against cloud account compromise and malicious files. We also protect against data theft and abuse of OAuth apps and IaaS resources. Our robust policies provide alerts and automated responses in real time. These help you suspend compromised accounts and quarantine malicious files. They also let you revoke malicious OAuth apps and remediate suspicious IaaS admin activity. And you can apply risk-based authentication and inline data controls.

When you deploy adaptive access controls, you can integrate your identity management solution through security assertion markup language (SAML) authentication. You can also integrate your multifactor authentication solution. Or you can use Proofpoint Mobile Access. Proofpoint Mobile Access is our mobile authenticator app. It is included with Proofpoint CASB.

Unify DLP Across Cloud Apps and Other Channels

Proofpoint CASB shares DLP classifiers with other Proofpoint products. These classifiers include built-in smart identifiers, dictionaries, rules and templates.

The sharing allows you to identify and protect sensitive data more quickly. And as part of the Proofpoint Information Protection solution, you can deploy consistent DLP policies across SaaS apps, IaaS buckets, email, web and endpoint. We combine content, behavior and threat telemetry from these channels. This helps you determine if the user who triggered the DLP alert is compromised, malicious or negligent. You can also unify DLP alert management for multiple channels in the Proofpoint Information and Cloud Security Platform.

About 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 than 240 built-in classifiers cover PCI, PII, PHI and GDPR regulations. Custom contextual rules and advanced detection technologies such as exact data matching also let you build your own DLP policies. And you can restrict data access from unmanaged devices, prevent sensitive file uploads to unapproved cloud apps and reduce sharing permissions for files and buckets. You can also correlate suspicious logins or misconfigured AWS S3 buckets with DLP incidents.

Govern Cloud and Third-Party Apps

Proofpoint CASB gives you visibility into shadow IT in your organization. We help you audit network traffic logs and discover cloud apps. Our catalog has 46,000 apps. And each app has more than 50 attributes. Cloud apps can be categorized by type and risk score. This helps you determine security risks, data loss vulnerabilities and non-compliance. You can block risky apps or grant users read-only access to them. We detect and assess OAuth permissions for third-party apps and scripts that access your IT-approved core cloud services. Our analysis helps identify risky apps and reduce your attack surface. You can define or automate actions based on risk score and context.

Centralize the management of multicloud and multiregion IaaS security and compliance. With a single console, you can discover approved and unapproved IaaS accounts and resources as well as identify misconfigurations and compliance issues.

Deploy Quickly With a Multimode Architecture

Our multimode architecture gives you unparalleled time to value. In less than four weeks, you can integrate with cloud-service APIs, hybrid identity management tools and security orchestration products (including Proofpoint Threat Response). This lets you automatically detect and contain threats as well as secure data. Risk-based SAML authentication and web isolation help prevent unauthorized access to corporate apps and enable BYOD strategies. With CASB Proxy and its lightweight endpoint agent, you can govern access to IT-approved and unapproved cloud apps and apply real-time DLP and threat protection as your people work anywhere.

For more on CASB, see proofpoint.com/us/products/cloud-app-security-broker.

For more information, visit proofpoint.com.