proofpoint.

DATA SHEET

Proofpoint Cloud App Security Broker

Gain Visibility and Control of Your Cloud Apps

KEY BENEFITS

- Protect cloud users with people-centric threat visibility and adaptive access controls for cloud apps
- Shorten time to discover and protect regulated cloud data with out-of-the-box DLP policies
- Protect sensitive data with accurate DLP that combines content, behavior and threat telemetry across cloud, email and endpoint channels
- Deploy stand alone or as part of our integrated Proofpoint Enterprise DLP solution
- Simplify multi-channel DLP operations with a unified alert manager that helps you quickly address data risks from negligent, compromised and malicious users (as part of Proofpoint Enterprise DLP)
- Discover cloud apps and contain shadow IT, including third-party OAuth apps
- Find 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

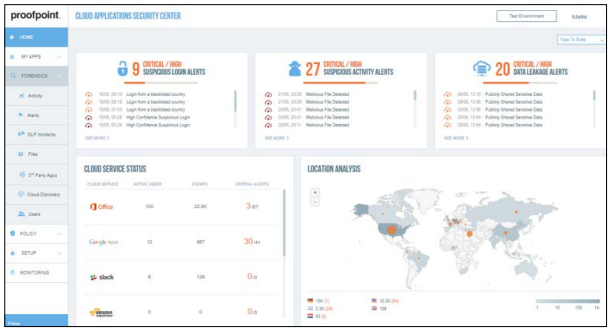
Proofpoint Cloud App Security Broker (Proofpoint CASB) takes a people-centric approach to protect your users from cloud threats and safeguard your sensitive data. It also helps you discover shadow IT and govern cloud and third-party OAuth apps.

Cloud security starts with safeguarding IT-approved apps that contain your most valuable data. These 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 your cloud apps, email and endpoint.

Proofpoint CASB protects you from:

- Account compromise
- Oversharing of data
- Misconfiguration of IaaS resources and compliance risks

Our agentless solution gives you people-centric visibility into threats, adaptive access controls, automated response and comprehensive data security with DLP. It also helps you govern SaaS and third-party apps and IaaS services for a stronger cloud security posture.



Extend people-centric visibility to cloud apps

Proofpoint CASB provides people-centric visibility into email and cloud threats. We help you Identify your Very Attacked People™ (VAPs) and protect their cloud accounts and data. What's more, you can see which files in your cloud apps are violating DLP rules, who owns them and who is downloading or sharing and editing them.

Our powerful 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 rich cross-vector (cloud, email and more) threat intelligence from Proofpoint Nexus Threat Graph with user-specific contextual data. Through machine learning and threat correlation, we help you detect when a cloud account is compromised.

In our intuitive dashboard, you can investigate alerts for suspicious login, file and administrative activities. You can also export forensics data manually or via REST APIs to a security information and event management (SIEM) solution for further analysis.

Without hindering user productivity, we protect against:

- Cloud account compromise
- Abuse of IaaS resources
- Data theft

And with our robust policies, you get alerts to issues in real time and automated response to risks:

- Remediate compromised accounts
- Quarantine malicious files
- Apply risk-based authentication when needed

When deploying adaptive access controls, you can integrate your identity management solution through security assertion markup language (SAML) authentication. You can also integrate your multi-factor authentication solution or use our mobile authenticator app—Proofpoint Mobile Access, which is included with Proofpoint CASB.

Unify DLP across cloud apps and other channels

Proofpoint CASB shares DLP classifiers—including built-in smart identifiers, dictionaries, rules and templates—with other Proofpoint products. So, you can:

- Start identifying and protecting sensitive data more quickly.
- Easily deploy consistent DLP policies across SaaS apps, IaaS buckets, email and endpoint. We combine content, behavior and threat telemetry from these channels to help you determine if the user who triggered the DLP alert is compromised, malicious or negligent.
- Unify DLP alert management for multiple channels in Proofpoint Enterprise DLP's alert manager.

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 allow you to build your own DLP policies. You can restrict data access from unmanaged devices, quarantine files and reduce sharing permissions for files and buckets.

We help you protect data at risk by identifying broad file permissions and unauthorized data sharing. You can 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 across your organization. We help you audit network traffic logs and discover cloud apps. Our catalog has 46,000 applications with more than 50 attributes per app.

The cloud apps can be categorized by type and risk score. This scoring 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 also detect and assess OAuth permissions for third-party apps and scripts that access your IT-approved core cloud services. Our in-depth analysis helps identify risky apps, including malicious ones, and reduces your attack surface. You can define or automate actions based on risk score and context.

Simplify multi-cloud and multi-region IaaS security and compliance with centralized management. With a single console, you can discover approved and unapproved IaaS accounts and resources, identify misconfigurations and compliance issues.

Deploy quickly with an agentless architecture

Our agentless architecture gives you unparalleled time to value. Powerful built-in features work with your existing cloud investments. It prevents, detects and remediates cloud threats quickly and automatically. Risk-based SAML authentication and web isolation help prevent cloud threats from the start. You can also integrate with cloud-service APIs, hybrid identity management tools and security orchestration products (including Proofpoint Threat Response) to detect and contain any threats that get through.

LEARN MORE AND SIGN UP FOR A FREE TRIAL

Visit **proofpoint.com/us/products/cloud-app-security-broker**.

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**.