DATA SHEET

PROOFPOINT CLOUD APP SECURITY BROKER

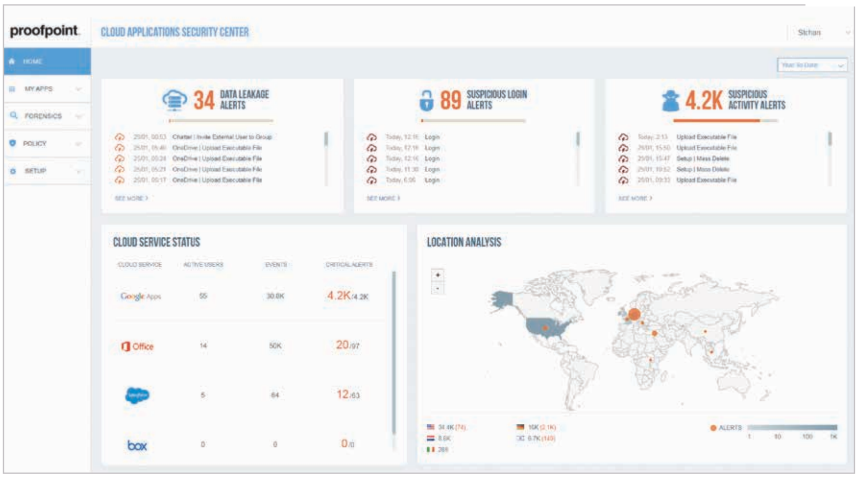
KEY BENEFITS

- Unique people-centred view of SaaS apps
- The best threat protection for SaaS apps, risk-based access control and analytics
- Threat-aware data security
- Third-party application control
- Vendor-neutral protection
- Automated policy-based response actions
- Award-winning customer support

Proofpoint Cloud App Security Broker (PCASB) protects people and data from advanced threats, accidental sharing and compliance risks in the cloud. With PCASB, you can deploy cloud apps and services with confidence. Our powerful analytics help you to grant the right levels of access to users and third-party apps based on the risk factors that matter to you.

Today's cyber-attacks target people and the way they work. Much of that work happens over cloud-based email and other SaaS apps such as Office 365, G Suite and Box. These apps contain sensitive data, and they connect to a wide range of third-party apps. This has made securing SaaS-hosted data more challenging and critical than ever. The path to better cloud application security lies in an integrated approach to threat detection that correlates threats across email and other cloud apps. Our integrated, people-centred solution helps you to prevent threats, safeguard your information and stay compliant.

USER-CENTRED VISIBILITY



25/01, 00:53 Chatter | Invite External User to Group
25/01, 05:40 OneDrive | Upload Executable File
25/01, 03:24 OneDrive | Upload Executable File
25/01, 05:21 OneDrive | Upload Executable File
25/01, 05:17 OneDrive | Upload Executable File

Today, 12:16 Login
Today, 17:16 Login
Today, 12:16 Login
Today, 11:30 Login
Today, 6:06 Login

Today, 2:13 Upload Executable File
25/01, 15:50 Upload Executable File
25/01, 15:47 Setup | Mass Delete
25/01, 10:52 Setup | Mass Delete
25/01, 09:33 Upload Executable File

CLOUD SERVICE	ACTIVE USERS	EVENTS	CRITICAL ALERTS
Google Apps	55	30.8K	4.2K/4.2K
Office	14	50K	20/97
salesforce	5	64	12/63
box	0	0	0/0

Security in the cloud begins with effective oversight of users and data. PCASB provides granular people-centred visibility to cloud access and data handling. You can view privileged accounts and stop them from multiplying. You can see which files in your SaaS apps are violating data loss prevention (DLP) rules, who owns them, and who is downloading or sharing them. And you can find answers to critical questions so that you can take action straight away.

PCASB brings together contextual data and behaviour analytics from users to determine suspicious activity. Context includes a user's location, device, network and any SaaS app the user is trying to access. For example, you can specify that only corporate devices that meet your end-point security standards can access a given SaaS app. You can limit permissions with read-only access or limit the data that the user can download.

PROVEN ADVANCED THREAT PROTECTION

A malicious file uploaded to a corporate SaaS app can spread instantly throughout your entire environment. Our sandboxing and analysis detect the potential risks posed by the SaaS apps in your environment. From there, PCASB helps you to contain them in real time through automated quarantine and other mitigation steps.

PCASB combines our rich cross-channel (SaaS, email and more) threat intelligence with user-specific risk indicators to analyse user behaviour and detect anomalies in SaaS apps. These anomalies include excessive activity, unusual access attempts and other issues.

Robust policy templates alert you to issues in real time, apply risk-based authentication and reduce privileges when needed. This prevents your data from being exposed, misused or deleted. You can also integrate existing identity-management solutions through SAML authentication. With our multi-mode architecture, you can enable protection through API or by forward and reverse proxy.

RISK-AWARE DATA SECURITY

As more of your organisation's data is stored in the cloud, so is sensitive content. PCASB shares DLP classifiers—which include built-in smart identifiers, dictionaries, rules and templates—with other Proofpoint products. These unified policies mean that you can identify and secure sensitive data faster.

Built-in classifiers cover PCI, PII, PHI and GDPR regulations. And flexible custom rules allow you to build your own DLP policies to control how your data is shared or downloaded. You can encrypt, mask or quarantine data, or utilise the context to stay compliant.

PCASB helps you to identify and protect data at risk because of broad permissions and unauthorised data sharing. Workers might be sharing company data with personal accounts, for example, or exporting large amounts of data. User-centred visibility and behaviour monitoring quickly reveals activity on orphaned and compromised accounts. Most importantly, PCASB correlates user-level risk indicators with DLP detection. This insight means that DLP alerts and changes to access control are more useful.

THIRD-PARTY APPS CONTROLS AND SHADOW IT

App marketplaces offer hundreds of third-party apps that can add more features to Office 365, G Suite, Box and other platforms. We provide a deep, vendor-neutral assessment to safeguard third-party apps and add-ons. If something appears risky, we provide complete transparency, objective identification and a timely response. We help you to keep users productive and limit their risk with the right level of visibility and control. In-depth analysis helps you to understand your risks on a per-app and per-user view.

Controls allow you to define or automate actions based on analysis results. Policies for privileged users help to define the permissions granted for an access token, such as read-and-write or read-only access. PCASB can also deny a request from an app that exceeds defined thresholds. You're always in control.

PCASB gives you visibility into Shadow IT across your organisation. We help you to audit network traffic logs and categorise cloud apps using risk scoring. This scoring helps you to determine the risk of data loss and non-compliance.

HOLISTIC PROTECTION

Using PCASB with Proofpoint Targeted Attack Protection for Email improves threat detection with cross-channel insights. Working together, the solutions correlate email-based attacks with unauthorised access and data leakage.

And using PCASB with the rest of Proofpoint Information Protection helps you to simplify data protection across cloud apps, email, on-premises file sharing and SharePoint. Shared data classifiers and templates help you to enforce consistent security and compliance policies across the digital enterprise.

FIND OUT MORE

Proofpoint Cloud App Security Broker helps you to deploy and use SaaS applications with confidence. Backed by our award-winning global support organisation, half of the Fortune 100 rely on us to protect their people, data and brands. Find out more and sign up for a free risk assessment at proofpoint.com/us/products/cloud-app-security-broker.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals to protect their users from the advanced attacks that target them (via email, mobile apps and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organisations of all sizes, including over 50 per cent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and utilise both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.