Forcepoint CASB

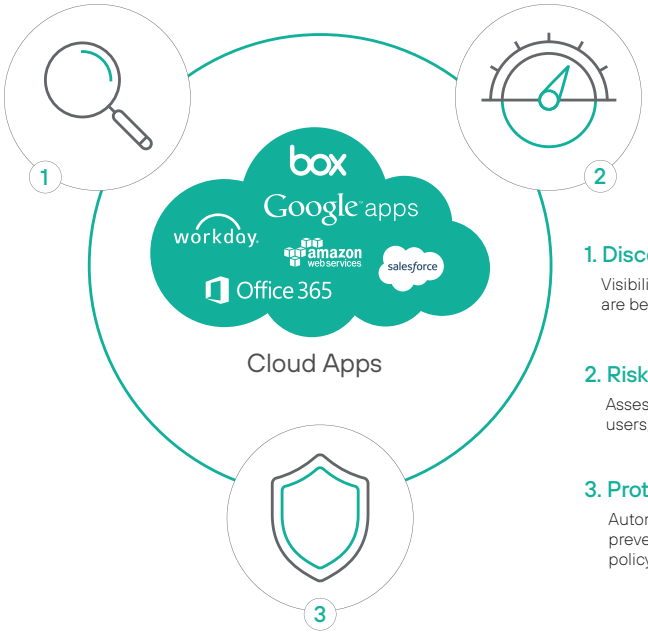
Discover cloud application use, analyze risk, and enforce appropriate controls for SaaS and custom applications

The Forcepoint CASB Value

- Discover and risk-prioritize all unsanctioned cloud use (Shadow IT) to quickly and easily determine if applications meet governance rules and avoid compliance issues
- Unleash the power of BYOD with improved employee productivity and cost savings while ensuring security of employees and corporate resources in the cloud
- Identify anomalous and risky user behavior in the cloud to stop malicious users, as well as clamp down on user activities that don't meet organizational standards
- Reduce the risk of exposing sensitive cloud data to unauthorized users in violation of governance and regulatory rules
- Identify potentially inappropriate privilege escalation to prevent the impact associated with root account takeover
- Implement geo-location-based access and activity monitoring for legitimate users and malicious actors
- Track application usage for compliance, licensing, and cost savings of unused accounts

Discover. Assess. Protect.

Forcepoint CASB offers enhanced security for data in cloud apps, so your end-users can access their favorite apps without restriction.



1. Discovery

Visibility into what apps are being used by employees

2. Risk Assessment

Assess contextual risk of apps, users, and security configurations

3. Protection & Control

Automated cloud threat prevention and context-aware policy enforcement

Forcepoint CASB provides visibility and control over both sanctioned and unsanctioned cloud apps.

Forcepoint CASB Solution Components — Cloud Governance | Cloud Protection | Cloud Security Suite

FEATURE GROUP	FEATURE DESCRIPTION	CLOUD GOVERNANCE	CLOUD PROTECTION	CLOUD SECURITY SUITE
Application Visibility & Risk	Cloud App Discovery — Leverage existing log files to automate discovery and categorization of cloud apps used	•		•
	Cloud App Risk Scoring — Rate overall risk for each cloud app based on regulatory and industry certifications and best practices	•		•
	Cloud App Usage Summary — Includes number of users, activities, traffic volume, and typical usage hours for each cloud application	•		•
	Adavanced Risk Metrics — Detailed cloud app risk posture metrics and information for each application	•		•
	Customizable Risk Metrics — Detailed cloud app risk posture metrics with customizable weightings	•		•
	Continuous Discovery — Schedule automated scanning of log files and generation of discovery reports on a periodic basis	•		•
	Centralized Discovery Dashboard — Aggregated discovery results, current usage baselined against prior activity, and usage trends	•		•
	App Catalog & Risk Updates — Automatic updates to cloud app catalog and changes in risk properties as they are available	•		•
	Activity Log Collections — Collect basic activity logs for users and privileged users via cloud app APIs	•		•
Account & Data	Data Classification — Identify and catalog sensitive or regulated data to ensure regulatory compliance (e.g., PCI, SOX, HIPAA, GDPR)	•		•
	User Governance — Identify inactive or orphaned accounts (e.g., ex-employees) and external users (e.g., contractors) to reduce operational costs/minimize security threats	•		•
	App Governance — Benchmark security configurations against a set of industry best practices/regulatory reqs. (e.g., PCI DSS, NIST, HIPAA)	•		•
	Integrated Remediation Workflow — Leverage built-in org. workflow to assign/complete risk mitigation via Forcepoint CASB or through third-party ticketing systems	•		•
Real-time Activity Monitoring & Analytics (available in inline/proxy)	Activity Monitoring & Analytics — Real-time activity monitoring and analytics by user, group, location, device, application action, and more		•	•
	Privileged User Monitoring — Real-time activity monitoring and reporting of privileged users and admins		•	•
	Enterprise SIEM Integration — Adaptors to directly feed activity logs into leading SIEM solutions, including ArcSight, Splunk, and Q1 Labs		•	•

Forcepoint CASB Solution Components — Cloud Governance | Cloud Protection | Cloud Security Suite

FEATURE GROUP	FEATURE DESCRIPTION	CLOUD GOVERNANCE	CLOUD PROTECTION	CLOUD SECURITY SUITE
Real-time Activity Monitoring & Analytics (available in inline/proxy)	Automatic Anomaly Detection — Continuously monitor behavior and detect anomalous activities, including high-risk insider and external attacks		•	•
	Real-Time Threat Prevention — Correlate activity anomalies with risky IP addresses to alert, block, quarantine, or verify ID for app or spec. within an app		•	•
	Data Leak Prevention — Data classification at rest and real-time content inspection for more than 100 file types and hundreds of pre-defined data types (e.g., PCI, PII, PHI, HIPPA, SOX)		•	•
	Multi-Factor Authentication — Risk-based identity verification when anomalous or high-risk activities are detected		•	•
	Single Sign-On — Leverage built-in or third-party SSO to access SAML-based apps		•	•
	Dynamic Alerts — Real-time notifications for policy violations or activity thresholds via SMS/email		•	•
	Mobile & Endpoint Access Control — Unique policies for managed and unmanaged devices, whether originating from browsers or rich mobile apps		•	•
	Location-Based Access Controls — Restrict access based on the location of the user or the location of the cloud service		•	•
	MDM Integration — Leverage existing MDM deployment to manage endpoint enrollment and cloud access		•	•
	Custom Policies — Visual policy editor enables easy configuration of custom policies based on various attributes		•	•
Advanced Cloud	Performance Optimization — Accelerate access to cloud apps through caching and content optimization	•	•	•
	Centralized Threat Intelligence — Unified view of threats to enterprise database tables, files stored in file shares, and data stored in cloud apps	•	•	•
Admin. & Access	SIEM Integration — Generate discovery data in Common Event Format for integration with existing SIEM environments	•	•	•
	Enterprise Directory Integration — Use existing AD or LDAP directory infrastructure for user, group, and organizational reporting and policy	•	•	•
	Role-Based Admin — Define permissions for editing assets, policies, and system settings	•	•	•
	Enterprise Reporting — Flexible reporting options including pre-defined reports with the ability to edit and save customized reports	•	•	•
	Encryption Broker – Bring your own key (BYOK) or encryption to cloud service providers, with Forcepoint CASB handling the key rotations and providing full audit			•

Forcepoint

Why Forcepoint CASB?

DLP Integration
Forcepoint CASB integrates with DLP solutions to provide unified data protection extending from on-premises to the cloud environment. It also integrates with solutions such as web security, email security, next-generation firewall, and more.

Built-in Cloud UEBA
Forcepoint CASB creates a risk profile based on threat likelihood and business impact. It utilizes analytics based on thousands of apps and activities to provide risk-prioritized alerts for SOC and incident response teams.

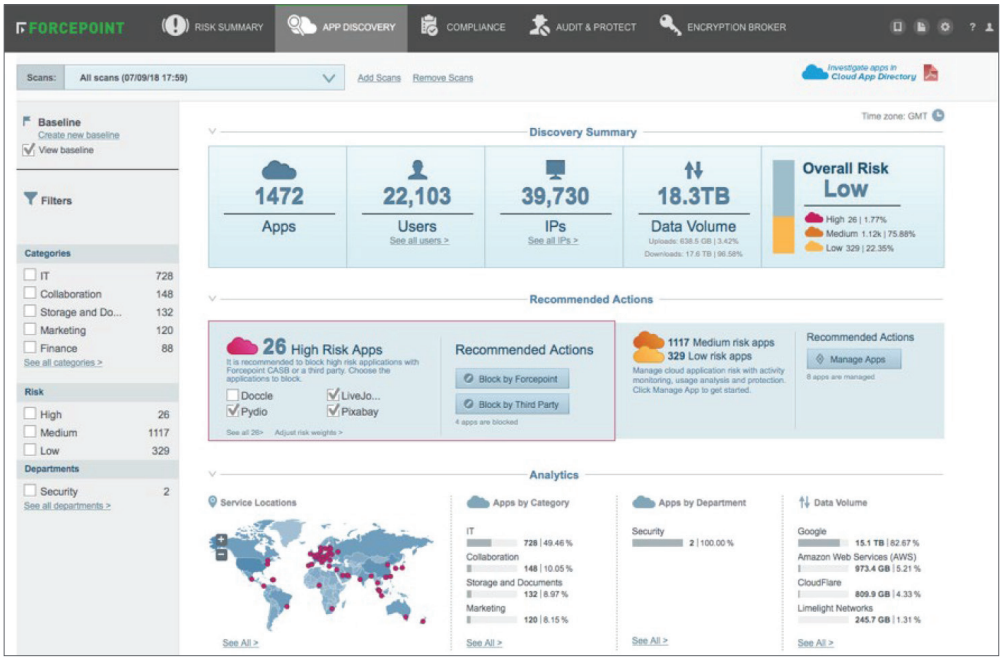
Bring Your Own Device (BYOD)
Forcepoint CASB has the most comprehensive use case coverage, with API and forward/reverse proxy support. This provides granular device and activity control for unmanaged devices.

Cloud Monitoring and Control for Any App
Forcepoint CASB has flexible product architecture to support any application, including custom applications, without product changes. Users can fully audit and protect application usage in a matter of hours or days.

Quick Time to Value
Choose from the best of both worlds with API and Proxy Mode to expedite implementation and reduce risk in your cloud environment.

Features and Benefits

- App Discovery, Governance, Compliance, Analytics, and Protection in one solution
- Deployment options for API and/or proxy mode
- Granular policies for mobile and endpoint devices enable access control and data protection for managed and unmanaged devices
- In-depth support for common apps (e.g., Office 365, AWS, Salesforce, Dropbox, G-suite, Box)
- Part of the Forcepoint ecosystem of products that span on-premises and cloud environments
- Integrate with enterprise directories, SIEM, and MDM
- Certified interoperability with Identity-as-a-Service (IDaaS) partners (e.g., Centrify, Ping, Okta)
- Extend anomaly and threat detection capabilities to cloud apps
- IP reputation data enables the creation and enforcement of more accurate risk-mitigation policies
- Analyze risk factors and compare apps side-by-side to find the best option for your cloud environment



forcepoint.com/contact

[FP-Datasheet-Template-US-EN] 21FEB2020

Forcepoint