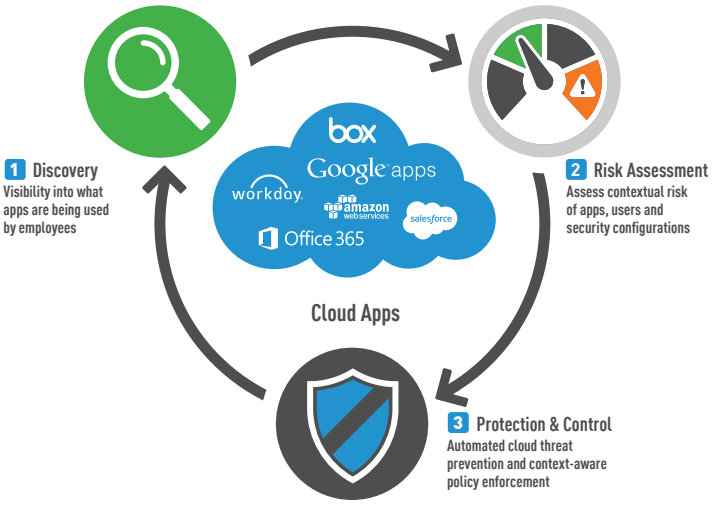
FORCEPOINT

Datasheet

FORCEPOINT CASB

Discovers cloud application use, analyzes the risks and enforces appropriate controls for SaaS and production applications.

Forcepoint Cloud Access Security Broker (CASB) automatically discovers cloud application use, analyzes the risks and enforces appropriate controls for SaaS and production applications. With Forcepoint CASB, users get the apps they want and IT staff gets the control they need.



Achieving visibility and control requires a cloud access security broker that supports app discovery, risk governance, access control and data protection for both sanctioned and unsanctioned apps.

Providing Visibility and Control Over the Use of Cloud Apps

Cloud apps allow organizations to reduce costs and elastically allocate resources—but also introduce risks to security and compliance posture. The acceleration of cloud app adoption in the workplace, along with the proliferation of BYOD, has created a need to secure cloud-based, sanctioned apps like Office 365, Dropbox and Salesforce. Preventing data loss and enforcing granular access controls are justifiably top of mind for IT.

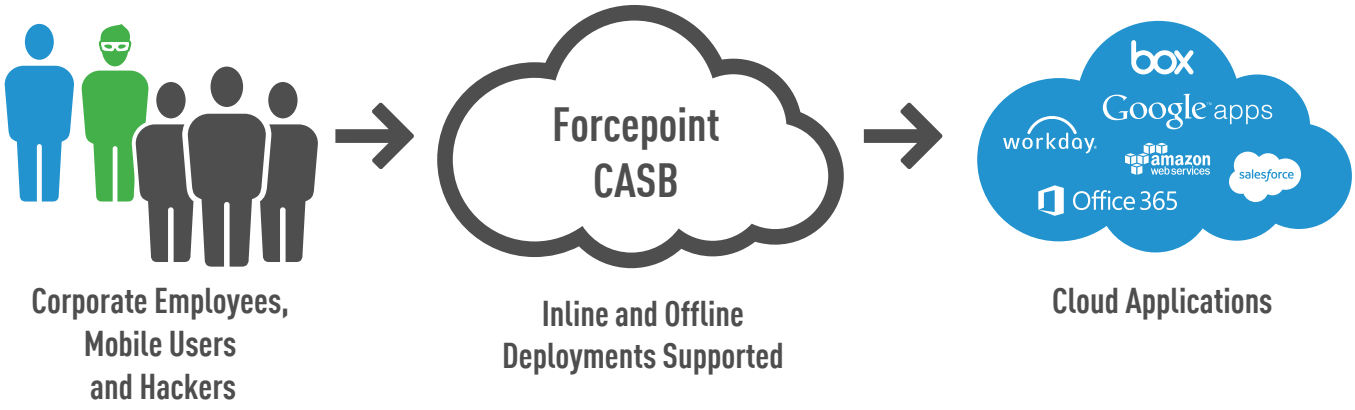
Employees can be a major source of security risk, as malicious insiders look to take advantage of their unfettered access to an organization's cloud apps to exfiltrate data.

Forcepoint ensures the safe and productive use of cloud apps across all users and endpoints.

Mitigating Cloud App Risk

Typically, organizations require visibility into cloud access before enforcing policies to eliminate or limit risk. That's why it's important to have a set of offline features to help you identify and assess your risk posture. Once you have investigated the threat landscape and created the required policies to address security risks, you can turn these offline features into inline solutions to actually enforce those policies. Gartner recommends solutions that offer the "best of both worlds" (i.e., a combination of proxies and APIs) in order to cover all the cloud security use cases for today's organizations.

* "Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, May 2017.



Forcepoint Cloud Access Security Broker provides visibility and control over both sanctioned and unsanctioned cloud apps.

Features and Benefits

- Part of the Forcepoint family of Cloud Security products that span on-premise and cloud environments
- Comprehensive App Discovery, Governance, Analytics and Protection in one integrated solution
- Deployment options for offline (API mode) and/or inline (proxy mode)
- Granular policies for mobile and endpoint devices enable access control and data protection for managed and unmanaged mobile phones, tablets, and laptops
- Built-in integration with enterprise directories, SIEM and MDM
- Deep support for Office 365, AWS, Salesforce, Google Apps, Box, Dropbox, NetSuite, Workday, Microsoft Azure and more
- Certified interoperability with Identity-as-a-Service partners: Centrify, Ping, Okta, OneLogin, SecureAuth, and Microsoft
- Extends an organization's anomaly and threat detection capabilities to cloud apps
- IP reputation data enables the creation and enforcement of more accurate risk-mitigation policies

Cloud Discovery and Governance

Forcepoint CASB extends traditional cloud app discovery information by providing details on risk factors that are unique and specific to your organization. For instance, Forcepoint CASB provides visibility into dormant (i.e., inactive) accounts, orphaned accounts (e.g., ex-employees) and external accounts (e.g., contractors) that present a variety of security risks.

Additionally, Forcepoint benchmarks your organization's cloud app security configurations against industry best practices and regulatory requirements, so that you can more easily pinpoint your security and compliance gaps and take action to remediate.

All of the Cloud Discovery & Governance features are enabled via a cloud app provider's APIs, an offline process that is non-intrusive and does not require any agents, changes to applications or logs to be sent outside your organization to Forcepoint.

Cloud Audit and Protection

Forcepoint CASB Cloud Audit and Protection delivers the operational intelligence and the tools you need to protect data in the Cloud and enforce comprehensive controls on user access. Forcepoint provides critical insight and intelligence into:

- **Data Loss Prevention for Data at Rest and Data in Transit:** Controls for sensitive and regulated data in the Cloud
- **User Monitoring:** Real-time activity monitoring & reporting of end users & admins
- **Cyber Threat Prevention:** Policy enforcement for alerting, blocking or requiring identity verification for any suspicious activities

Forcepoint CASB monitors and controls uploads, downloads and sharing of sensitive data based on various criteria such as by destination, user or cloud app. Moreover, it scans your corporate data stored in file-sync services like OneDrive and Box, highlighting those files that are sensitive or regulated so that you can apply the appropriate policy (e.g., send an alert) to mitigate risk.

Forcepoint CASB inspects files and content in real-time to ensure that your PII, PCI, HIPAA and other sensitive information stays protected. Administrators can choose to quarantine files, remove the sensitive files from the cloud repository and notify end users. A copy of the file can also be added to a trusted folder for further review. Forcepoint CASB offers built-in data loss prevention (DLP) or standard ICAP-based integration with leading DLP solutions so that you can leverage existing data protection policies.

Forcepoint CASB automatically detects and blocks threats to cloud applications and enforces risk-mitigation policies. Through unique fingerprinting techniques, Forcepoint CASB quickly establishes detailed behavioral profiles based on the normal usage patterns for each user, department and device. Any access that fails the fingerprint test can be configured to immediately alert, block or require two-factor authentication in real-time. You can also quickly create custom policies and enforce them across selected cloud apps.

Forcepoint CASB enables you to block or restrict cloud app access from unmanaged endpoints (e.g., BYOD or personally owned devices), providing a cost-effective alternative to routing all remote access through a VPN. Additionally, Forcepoint CASB has built-in adaptors that make it easy to integrate with enterprise directories and market-leading SIEM solutions.

Forcepoint CASB — Product Feature Comparison

FEATURE GROUP	FEATURE DESCRIPTION	Cloud Governance	Cloud Audit & Protection	Cloud Security Suite
Application Visibility & Risk Assessment (available in offline/API)	CLOUD APP DISCOVERY — Leverage existing log files to automate discovery & categorization of cloud apps used	●		●
	CLOUD APP RISK SCORING — Rate overall risk for each cloud app based on regulatory & industry certifications & best practices	●		●
	CLOUD APP USAGE SUMMARY — Includes number of users, activities, traffic volume and typical usage hours for each cloud application	●		●
	ADVANCED 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	●		●
	SIEM INTEGRATION — Generate discovery data in Common Event Format for integration with existing SIEM environments	●		●
	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 Governance (available in offline/API)	DATA CLASSIFICATION — Catalog and identify sensitive or regulated data, including sharing permissions for each file, stored in file-sync services to ensure compliance with regulations such as PCI, SOX, and HIPAA.	●		●
	USER GOVERNANCE — Identify dormant (i.e., inactive) accounts, orphaned accounts (e.g., ex-employees), and external users (e.g., contractors) to reduce operational costs & minimize associated security threats	●		●
	APP GOVERNANCE — Benchmark your cloud app security configurations against a set of industry best practices & regulatory requirements (e.g., PCI DSS, NIST, HIPAA, CJIS, MAS, ISO) to identify security & compliance gaps	●		●
	INTEGRATED REMEDIATION WORKFLOW — Leverage a built-in organizational workflow to assign and complete risk mitigation tasks via Forcepoint CASB or through integration with 3rd-party ticketing systems	●		●

Forcepoint CASB — Product Feature Comparison (continued)

FEATURE GROUP	FEATURE DESCRIPTION	Cloud Governance	Cloud Audit & Protection	Cloud Security Suite
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		●	●
	ENTERPRISE DIRECTORY INTEGRATION — Use existing AD or LDAP directory infrastructure for user, group, and organizational reporting and policy		●	●
	ROLE-BASED ADMINISTRATION — Define admin permissions for editing assets, policies, & system settings		●	●
	ENTERPRISE REPORTING — Flexible reporting options including pre-defined reports with ability to edit and save customized reports		●	●

[1] Optional, add-on product to the base Forcepoint CASB license, purchased separately.

CONTACT
www.forcepoint.com/contact

[DATASHEET_FORCEPOINT_NEXTGENERATIONFIREWALL_EN] 100055.021518