FORCEPOINT CASB—PRODUCT FEATURE COMPARISON

		FORCEPOINT PRODUCTS		
FEATURE GROUP	**FEATURE DESCRIPTION**	**CLOUD GOVERNANCE**	**CLOUD AUDIT & PROTECTION**	**CLOUD SECURITY SUITE**
Application Visibility & Risk Assessment (available in offline/API deployments)	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 deployments)	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	●		●
	ADVANCED MALWARE PROTECTION— Identify today's evasive malware hidden in files stored in cloud storage and block or quarantine accounts that could lead to crippling breaches.	●		●

		FORCEPOINT PRODUCTS		
FEATURE GROUP	**FEATURE DESCRIPTION**	**CLOUD GOVERNANCE**	**CLOUD AUDIT & PROTECTION**	**CLOUD SECURITY SUITE**
Real-time Activity Monitoring & Analytics (available in inline/proxy deployments)	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		●	●
Account & Data Governance (available in offline/API deployments)	AUTOMATIC ANOMALY DETECTION—Continuously monitor behavior & detect anomalous activities, including high-risk insider and external attacks		●	●
	REAL-TIME THREAT PREVENTION—Correlate activity anomalies with risky IP addresses.[1] Apply policy to alert, block, quarantine, or require identity verification for any app or specific action within the 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 that meet the requirements of a range of regulations (e.g., PCI, PII, PHI, HIPAA, SOX)		●	●
	MULTI-FACTOR AUTHENTICATION—Risk-based identity verification (e.g., one-time passcode sent to a user's mobile device) when anomalous or high-risk activities are detected		●	●
	SINGLE SIGN-ON—Leverage built-in SSO or 3rd-party solution to access SAML-based apps		●	●
	DYNAMIC ALERTS—Receive real-time notifications for policy violations or activity thresholds via SMS/email		●	●
	MOBILE & ENDPOINT ACCESS CONTROL—Enable unique policies for managed & 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		●	●

		FORCEPOINT PRODUCTS		
FEATURE GROUP	**FEATURE DESCRIPTION**	**CLOUD GOVERNANCE**	**CLOUD AUDIT & PROTECTION**	**CLOUD SECURITY SUITE**
Advanced Cloud Architecture	PERFORMANCE OPTIMIZATION—Accelerate access to cloud apps through the caching and content optimization features of a world-class content delivery network with over 30 data centers globally		●	●
	CENTRALIZED THREAT INTELLIGENCE—Unified view of anomalies and threats to enterprise database tables, files stored in file shares, and data stored in cloud apps		●	●

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

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_FORCEPOINT_CASB_PRODUCT_FEATURE_COMPARISON_CHART_EN] 100056.061617