DATASHEET

TrustLayer Cloud Application Security

Cloud application security from TrustLayer provides a single pane of glass to discover, analyze and manage cloud activity across multiple networks and devices, whether users are on the corporate network or working remotely.

CASB is fully integrated with the TrustLayer Platform that also includes Email Security, Web Security and Multi-Factor Authentication. The TrustLayer Platform provides a single web interface for central policy configuration and management, as well as data visualization and reporting.

CASB inline mode is deployed using agents or proxies, or a combination of both, to meet the needs of organizations of all sizes. This flexible architecture significantly reduces the effort involved in implementing and managing the solution, accelerating time to value.

Using purely agents on endpoints, CASB offers a proxy-less approach which significantly reduces latency, preserves the user's real IP address and maintains privacy by allowing the browser to maintain direct communication with the cloud application server.

Users enjoy a fast, unobtrusive experience and the freedom to work however, whenever and wherever they want - with a consistent experience regardless of the device used. IT maintain visibility and where appropriate, control.

Agents can be used in combination with the TrustLayer Cloud Gateway for sites with populations of fixed desktops, such as call centers. Installing a single gateway rapidly extends security policies to the entire network.

API mode uses API connectors to major cloud storage applications including box, Dropbox and Microsoft OneDrive. API mode extends visibility of user activity to include mobile access using mobile apps (outside the browser)

CLOUD APP CONTROL

- Provides discovery and visibility of all cloud applications in use
- Inline and API 'multimode' CASB solution maximises visibility and protection
- Secures sanctioned cloud services such as Salesforce, Office365 and Box –enabling safe cloud adoption
- Protects against malware and other cloud threats using multiple security layers and a powerful combination of technologies
- Complete visibility – including deep inspection of SSL encrypted traffic
- Dedicated team constantly update the TrustLayer Cloud Application Catalog covering thousands of actions across hundreds of cloud applications
- Applications are risk assessed, rated and categorized with the ability to override pre-defined ratings
- Policies can be set at a granular level based on the individual or role, the device being used, the network connected to, the function within the application and the location of the user
- Flexible deployment options – agent or proxy, or both
- Agents for Microsoft Windows and MAC OS X
- Mobile device coverage by routing traffic (via VPN) through the TrustLayer Cloud Gateway, on premise or in the Cloud, or using API mode

API mode also includes the ability to scan files on upload and change for specific content - using predefined DLP templates - as well as scanning files for malware. Policy templates are included for Personal Identifiable Information, Intellectual Property, Confidential Information, Insider Risk, PCI DSS, and HIPAA. Additional keyword lists can be created if required.

API mode works by linking the TrustLayer CASB to corporate accounts in supported cloud storage applications and can be used standalone (without the need for agents or gateways) or in combination with Inline mode.

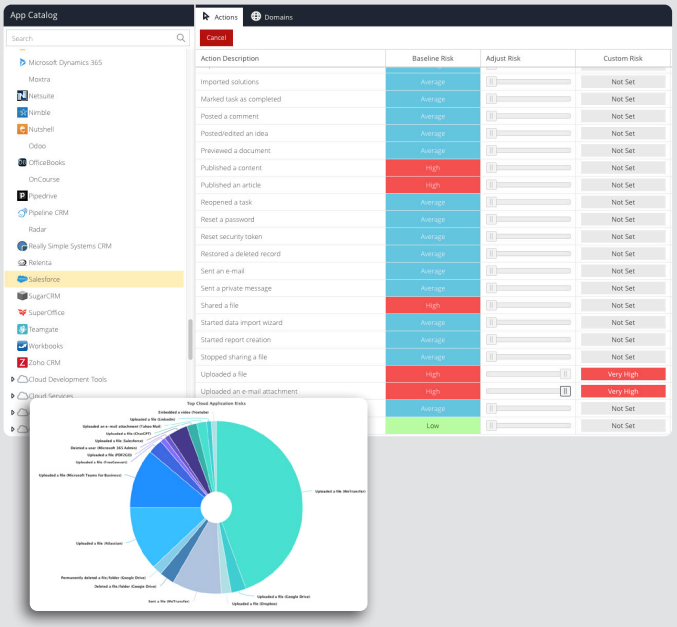
A sophisticated policy engine enables rules that audit or manage access to applications as well as user actions within applications. Generic activities can be blocked across all apps, apps within one or multiple classes, or specific apps. Conditions further refine rules to limit control by user, device, network, time, or risk level. Rules may also be triggered based on content – such as the email address used to login or keywords within social media posts.

At the heart of the CASB service is the TrustLayer Cloud Application Catalog that contains constantly updated, detailed information about thousands of features within hundreds of cloud apps.

Applications are categorized into classes (e.g. Cloud CRM, Cloud Storage, Social Media) risk assessed and rated. Pre-defined ratings can be easily modified to reflect an organisation's overall risk appetite, specific concerns or to align with expected user activity in particular roles.

CASB is fully integrated with the TrustLayer Platform portal provides rich data visualization and reporting across an extensive set of attributes and criteria. Analysis and reporting is available by time, user, device, app class, app name, app action, keywords, risk level and outcome (block or allow).

Whether audit data is required purely for visibility into the use of unsanctioned applications (or Shadow IT), or to under-stand the extent of personal mobile device use (BYOD), or for more formal attestation of compliance with internal policies or external standards, regulations and legislation, Cloud Application Security will provide the evidence needed.



KEY FEATURES

Cloud App Discovery	• Detect cloud application usage and activity and reveal which applications are in use – including applications that use a custom domain. • Applications within the catalog are risk assessed, rated and categorized with the ability to override pre-defined ratings. Vendor profiles provide information on revenue/size for increased confidence when sanctioning apps.
Application Control	• Control access to applications at a granular level – down to individual features and actions within applications. • Block generic activities across all apps (e.g. File Upload, Share File), app class (CRM, Social Media, File Storage), or specific apps. Apply conditions to limit control by user, device, network, time, risk level. • Block actions based on content such as email address used to login, or keywords within social media posts.
Anti-Malware Scanning	• Incorporates multiple security layers each using a powerful and effective combination of tools and techniques including on-line threat detection, reputation and heuristics.
HTTPS Inspection	• Deep HTTPS inspection allows SSL encrypted content to be scanned for malware (requires TrustLayer Cloud Gateway on premise or in the Cloud). • Ability to disable SSL inspection for specific trusted apps.
Anonymous Proxy Detection	• Prevent access to anonymous proxy sites.

MANAGEMENT

Policy Engine	• Sophisticated policy engine including AzureAD attributes, IP, MAC address, device type, custom tags, and differential actions.
Time Schedule	• Policies can be applied on a rolling 7-day schedule to customise access restrictions.
User Authentication and Synchronisation	• Multiple authentication methods supported including AD Kerberos, SSO, Captive Portal and RADIUS accounting. AD sync service ensures changes are replicated seamlessly.
Web Portal	• Fully integrated with TrustLayer's other modules, the CloudUSS dashboard offers a single pane of glass interface for management and reporting.
Delegated Admin	• Full Role-Based Access Control (RBAC) enables a range of access profiles and control/ visibility permissions.
Custom Notifications	• Customise and brand notification and block pages with logo, html text, and other useful user information.

REPORTING

Real-time Visibility	• Multiple charts and tables give instant insights on your user activity. Query the logs in realtime by numerous filter attributes to see exactly which users are accessing which sites.
Curated Reports	• Admins can build their own reports based on available fields and criteria, and can then export via PDF. • Audit reports can be searched using criteria including time, user, device, app class, app name, app action, keywords (e.g. filename, comment, log in details), risk level, threat type (API mode), policy name, outcome (block or allow).
Shceduling and Alerting	• Link curated reports to a delivery schedule so analytics can be delivered to email inboxes on a regular cadence.
Interactive Reports	• Charts and Tables in the portal are fully interactive enabling admins to go from high-level trends to forensic-level detail with just a few clicks enabling prompt incident response.
Log Retention	• Web Security log data is archived automatically after 30 days. Log Streaming functionality is available to send logs to a 3rd party SIEM tool in realtime.

DEPLOYMENT

Agent (Inline CASB)	• Agents for Microsoft Windows and MAC OS X enforce policies on the device. Tamper proof and easy to deploy using an install wizard or via AD Group Policy.
Gateway (Inline CASB)	• TrustLayer Cloud Gateway can be installed on a virtual machine or physical server within 30 minutes to extend security policies to the entire network. Also available in the Cloud.
API Mode	• Cloud-based API gateway with API connectors to common cloud storage apps. Link corporate accounts in supported applications and optionally scan files for content (DLP scanning) and/or malware. • Categories supported include Gore, Adult, Underwear (inc. swimwear) and Extremism. • Apps supported include box, Dropbox, Google Drive, Microsoft OneDrive and SharePoint.