

Cloud Application Security

See and control every cloud app in use.

A single pane of glass to discover, analyse and manage cloud activity across every network and device, whether users are on the corporate network or working remotely.

THREE WAYS TO DEPLOY

Inline, gateway or API. Multimode by design.

Deploy with agents or proxies, or a combination of both, to meet the needs of organisations of all sizes. This flexible architecture cuts the effort of implementing and managing the solution, accelerating time to value.



ENDPOINT-ENFORCED

Inline agent

- Tamper-proof agents for Microsoft Windows and MAC OS X enforce policy on the device, deployed via install wizard or AD Group Policy.
- A purely agent-based approach is proxy-less: it cuts latency, preserves the user's real IP address and lets the browser talk directly to the cloud app.



NETWORK-WIDE

Cloud gateway

- Install on a VM or physical server in 30 minutes to extend policy across the entire network, ideal for sites of fixed desktops such as call centres.
- Also available in the Cloud, and routes mobile device traffic via VPN, on premise or in the Cloud.



AGENTLESS COVERAGE

API mode

- Connects to box, Dropbox, Google Drive, OneDrive and SharePoint to extend visibility to mobile apps outside the browser.
- Scans files on upload and change for content (DLP) and malware. Runs standalone with no agents or gateways, or combined with inline.

Enabled instantly, no additional hardware, software or configuration changes. Fast and unobtrusive for users, while IT keep visibility and control.

POLICY ENGINE

Rules that fit how people actually work.

The policy engine audits or manages access to applications and user actions within them. Block generic activities across all apps, one or more classes, or specific apps, and trigger on content such as the login email or keywords in social posts. For file scanning, policy templates are included for Personal Identifiable Information, Intellectual Property, Confidential Information, Insider Risk, PCI DSS and HIPAA, and additional keyword lists can be created if required. Every rule refines by:

User

Role

Device

Network

Location

Time

Risk level

App function

Content

CLOUD APP CONTROL

Discover. Control. Protect.

An inline and API 'multimode' solution that maximises visibility and protection across sanctioned and unsanctioned cloud, without frustrating users.



Discover

- ✓ Discovery and visibility of every cloud application in use
- ✓ A dedicated team constantly update the TrustLayer Cloud Application Catalog, covering 8,000+ actions across 2,000+ cloud applications
- ✓ Applications are risk assessed, rated and categorised, with the ability to override pre-defined ratings



Control

- ✓ Inline and API 'multimode' solution to maximise visibility and protection
- ✓ Granular policy by individual or role, device, network, application function and user location
- ✓ Flexible deployment: agent or proxy, or both, with agents for Microsoft Windows and MAC OS X
- ✓ Mobile device coverage via VPN through the TrustLayer Cloud Gateway, on premise, in the Cloud, or using API mode



Protect

- ✓ 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 technologies
- ✓ Complete visibility, including deep inspection of SSL encrypted traffic

2,000+

cloud apps in the catalog

8,000+

actions risk-rated

6

built-in DLP templates

30 min

gateway deployment

THE APPLICATION CATALOG

Thousands of apps, constantly rated.

At the heart of the CASB service is the TrustLayer Cloud Application Catalog: constantly updated, detailed information on thousands of features within 2,000+ cloud apps.

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

Analysis and reporting spans time, user, device, app class, app name, app action, keywords, risk level and outcome (block or allow), whether for Shadow IT visibility, BYOD, or formal compliance attestation.

TrustLayer Platform · App Catalog

App Catalog

Actions

Domains

Search

Cancel

Action Description	Baseline Risk	Adjust Risk	Custom Risk
Imported solutions	Average	1	Not Set
Marked task as completed	Average	1	Not Set
Posted a comment	Average	1	Not Set
Posted/edited an idea	Average	1	Not Set
Previewed a document	Average	1	Not Set
Published a content	High	1	Not Set
Published an article	High	1	Not Set
Reopened a task	Average	1	Not Set
Reset a password	Average	1	Not Set
Reset security token	Average	1	Not Set
Restored a deleted record	Average	1	Not Set
Sent an e-mail	Average	1	Not Set
Sent a private message	Average	1	Not Set
Shared a file	High	1	Not Set
Started data import wizard	Average	1	Not Set
Started report creation	Average	1	Not Set
Stopped sharing a file	Average	1	Not Set
Uploaded a file	High	1	Very High
Uploaded an e-mail attachment	High	1	Very High
Used a search engine	Average	1	Not Set
Used two factor authentication	Low	1	Not Set

Baseline and custom risk, adjustable per action.

KEY FEATURES

What you get out of the box.



Cloud App Discovery

Detect usage and activity, including apps on custom domains. Catalog entries are risk assessed and rated, with vendor profiles showing revenue/size for confident sanctioning.



Application Control

Granular control down to individual features and actions. Block generic activities (e.g. File Upload, Share File) across all apps, an app class (CRM, Social Media, File Storage), or specific apps, and by content such as login email or social keywords.



Anti-Malware Scanning

Multiple security layers combining online threat detection, reputation and heuristics.



HTTPS Inspection

Deep HTTPS inspection scans SSL encrypted content for malware (via the TrustLayer Cloud Gateway), with the ability to disable inspection for trusted apps.



Anonymous Proxy Detection

Prevent access to anonymous proxy sites.

DEPLOYMENT

Deploy your way

Agent (Inline CASB)

Agents for Microsoft Windows and MAC OS X enforce policies on the device. Tamper proof and easy to deploy via install wizard or AD Group Policy.

Gateway (Inline CASB)

TrustLayer Cloud Gateway installs on a VM or physical server within 30 minutes to extend security policies network-wide. Also available in the Cloud.

API Mode

Cloud-based API gateway with connectors to common cloud storage apps. Link corporate accounts and optionally scan files for content (DLP) and/or malware. Categories supported include Gore, Adult, Underwear (inc. swimwear) and Extremism. Apps supported include box, Dropbox, Google Drive, Microsoft OneDrive and SharePoint.

Central control

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.
Authentication & Sync	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 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

Evidence on demand

Real-time Visibility	Multiple charts and tables give instant insight. Query logs in realtime by numerous filter attributes to see exactly which users access which sites.
Curated Reports	Build reports from available fields and criteria and export via PDF. Search audit reports by time, user, device, app class/name/action, keywords (e.g. filename, comment, log in details), risk level, threat type (API mode), policy name and outcome (block or allow).
Scheduling & Alerting	Link curated reports to a delivery schedule so analytics reach email inboxes on a regular cadence.
Interactive Reports	Fully interactive charts and tables take admins from high-level trends to forensic detail in a few clicks for prompt incident response.
Log Retention	Web Security log data is archived automatically after 30 days. Log Streaming can send logs to a 3rd party SIEM tool in realtime.

PART OF THE TRUSTLAYER PLATFORM

Cloud Application Security is part of the Browse layer. Eight solutions, four layers, one platform.



Browse

Web

CASB

AI Exposure



Posture

CSPM

SSPM



Mail

Email

Archiving



Users

SAT