Cloud Application Security (CASB)

Cloud application security from Censornet 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 Censornet's lat o that also includes Email Security, Web Security and Multi-Factor Authentication. n o n t lat o 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 Censornet 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 APPLICATION SECURITY

- 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 Censornet Cloud Application Catalog covering thousands of functions / actions in 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 Censornet 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.

Image Analysis scans image files on upload and change for inappropriate 'Not Safe For Work' (NSFW) content.

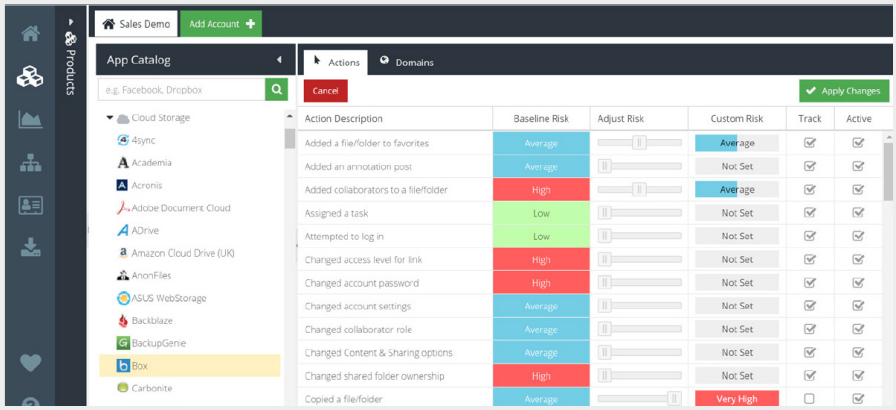
API mode works by linking Censornet CASB to corporate accounts in supported cloud storage applications and can be used standalone (without the need for agents or gateways) or in combination with Inline mode.

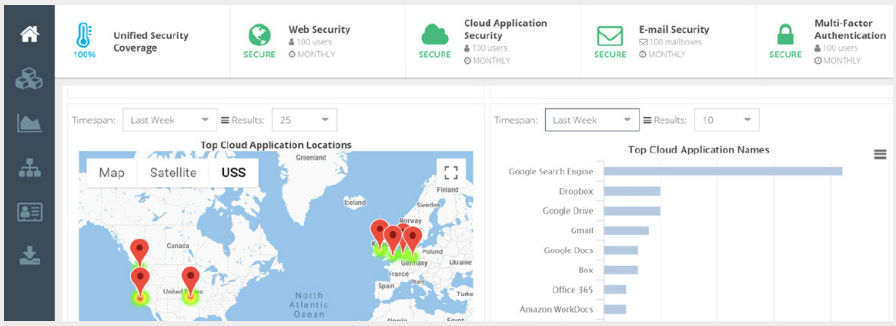
A sophisticated policy engine enables rules that audit or manage access to applications as well as user actions within applications. Generic activities can be blocked across all apps, apps within one or multiple classes, or specific apps. Conditions further refine rules to limit control by user, device, 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 Censornet 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 Censornet lat o 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 understand 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 Application 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.
Cloud 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.
Real-time 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 Censornet 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 Active Directory attributes, device IP and MAC address, device type, tag, and differential actions.
Time Schedule	• Policies can be applied on a rolling 7-day time schedule.
User Authentication	• Multiple authentication methods are supported including Active Directory Kerberos, single-sign-on, Captive Portal and RADIUS accounting.
User Synchronization	• Active Directory synchronisation service ensures changes to Active Directory are replicated.
Web Interface	• Fully integrated with the Censornet lat o
Delegated Administration	• Allows creation of multiple administrators with different levels of access to the n o n t lat o

REPORTING

Real-time Visibility	• Productivity charts display instant visibility on compliance with defined access policies. • Query in real time web activity by user, domain, application and category. See exactly which users are accessing which applications – and features within those applications.
Report Builder	• Administrators can define their own reports based on available field names and criteria. Reports can be saved and then exported to CSV or 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).
Scheduling and Alerting	• Link reports to schedules and optionally only receive a report when there is content (alert mode). Alert on high risk actions, keywords, allowed activity etc.
Top Trend Reports	• A selection of pre-defined trend reports with chart and table data. Trend reports can be exported to PDF and e-mailed to recipients.
Multiple Views	• Analyse and report by user, application, device, feature/action, threat level and detail (API mode).

DEPLOYMENT

Gateway (Inline mode)	• Censornet 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.
Agents (Inline mode)	• 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.
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. • Optional Image Analysis scans image files for inappropriate Not Safe For Work (NSFW) content. • Categories supported include Gore, Adult, Underwear (inc. swimwear) and Extremism. • Apps supported include box, Dropbox, Google Drive, Microsoft OneDrive and SharePoint.
Deployment Modes	• Agent software, direct proxy (set by group policy, WPAD or manually), or gateway mode for guest, personal (BYOD) or non-domain devices.
WPAD Support	• Automatic creation of Web Proxy Automatic Discovery (WPAD) file based on network configuration.
WCCPv2 Support	• Supports Web Cache Communication Protocol (WCCP)v2 for transparent traffic redirect from Cisco routers / switches.

censornet.

E. EMAIL

Secure your entire organization from known, unknown & emerging email security threats - including email fraud.

S. SAT

Defend your organisation against cybercriminals by strengthening your engaging and stimulating automated training.

W. WEB

Protect users from webborne malware, offensive or inappropriate content & improve productivity.

C. CASB

Discover, analyze, secure & manage user interaction with cloud applications - inline & using APIs.

M. MFA

Reduce impact of large scale data breaches by protecting user accounts with more than just passwords.

ID. IDaaS

Control user access with complete identity-threat protection. Automatically authenticate users using rich contextual data.

Our Platform

Our cloud security platform integrates email, web, and cloud application security, working seamlessly with powerful identity management to activate the Autonomous Security Engine (ASE).

This takes you beyond alert driven security and into real-time automated attack prevention.

Autonomous Security Engine

Enable traditionally silo'd products to share and react to security events and state data whilst

leveraging world class threat intelligence. Prevent attacks before they enter the kill chain.

ASE provides 24x7 security so you don't need to.

Full access to threat intelligence without the cost.

Integral part of the Censornet Platform.

CENSORNET LTD

Matrix House, Basing View, Basingstoke, RG21 4DZ, UK

Phone: +44 (0) 845 230 9590

CENSORNET LTD

Park Allé 350D, 2605 Brondby, Denmark

Phone: +45 61 80 10 13

CENSORNET LTD

700 Lavaca Street Suite 1400-PMB#100122 Austin, TX 78701

Phone: +1 (877) 302-3323