



Censornet Platform

Freedom. Visibility. Protection. The Censornet Platform from Censornet fully integrates Email, Web, and Cloud Application Security (CASB) with Identity (IDaaS) and Multi-Factor Authentication (MFA) for both central configuration and management, as well as data visualization and reporting.

The Censornet Platform provides a single pane of glass view across multiple critical solutions, simplifying security, architected specifically and equally for both enterprises and MSPs.

Organizations to move away from the more expensive approach of running separate solutions in silos with the Censornet Platform. Security teams are able to effectively and efficiently manage core security defenses, in a way that reflects how modern enterprises work today.

With the Censornet Platform, users are allowed the freedom to access the applications and data they need - regardless of device or location, whilst providing visibility for IT and protection for all.

CENSORNET PLATFORM

- Fully integrates multiple core security services for simplified management with a single underlying shared identity store
- 100% cloud-based with the ability to specify data residency by region (US, UK, Europe) per account
- REST API for inclusion of any element of the Censornet Platform interface in virtually any other application
- Define unlimited administrator roles for flexible segregation of the admin function
- Comprehensive audit trail of all administrator activity
- Home Dashboard with a range of charts and graphs for each service - for instant visibility of key metrics and trends
- Detailed reporting and analysis by an extensive list of drill-down criteria - including time, user, device, URL category, cloud application class, high risk actions, keywords, policy name, email volume, spam, malware and more
- Link reports to schedules to send via email as CSV or PDF attachment - also used for email alerts
- Auto-archiving of log data as well as scheduled reports
- Fully integrates with Microsoft® Active Directory (if required)
- Included with the purchase of any Censornet service - add additional services at any time

E.
EMAIL

Secure businesses from known, unknown & emerging email threats - including email fraud

W.
WEB

Protect your users from web-borne malware, offensive or inappropriate content & improve productivity

C.
CASB

Discover, analyse, secure & manage user interaction with cloud apps - inline using APIs

M.
MFA

Reduce impact of large-scale data breaches by protecting users' accounts with more than just a password

ID.
IDaaS

Secure access to cloud applications with Single Sign-On for users

S.
SAT

Strengthen your 'human firewall' with engaging, automated training and realistic phishing simulations

← **DLP** Secure sensitive data against loss or misuse →

← **ASE: Autonomous Security Engine**

Enables our core services to share security event and state data and react in real time, whilst leveraging world class threat intelligence, to stop multi-channel attacks →

Preventative

| Threat Intelligence

| Enterprise DLP

| Geolocation

| Unified Policy Engine

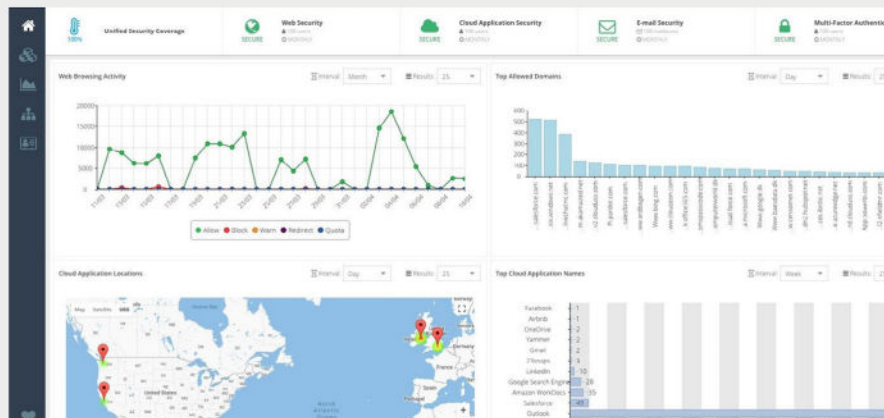
| UEBA

DASHBOARDS & REPORTING

The Censornet Platform provides rich data visualization and reporting across all Censornet services and an extensive set of attributes and criteria.

Each administrator has their own Home Dashboard with charts and widgets specific to the services licensed. Multiple standard reports are included for each service within the Analytics section of the portal.

Detailed analysis and reporting is available by time, user, device (hostname and MAC address), URL category, web category, cloud application class, cloud app name, cloud app action, keyword (e.g. filename, comment, login details), policy name, risk level, email direction, delivery status (delivered, spam, virus), outcome (block or allow).



To optimize storage and reporting speeds logs are auto-archived based on individual service retention periods. As standard, these are 90 days for Email and Web Security and 1 year for Cloud App Security and MFA. Archives can be downloaded on-demand in CSV format.

Whether audit data is required purely for visibility or for more formal attestation of compliance with internal policies or external standards, regulations and legislation, the Censornet Platform will provide the evidence needed.

IDENTITY INTEGRATED

The Censornet Platform provides the flexibility to create unlimited admin roles based on over 100 access controls with the option to protect administrator accounts with two-factor authentication.

The admin function can be split to match organizational requirements, segregating account and agent provisioning, from viewing web usage reports, from maintaining URL categories or managing the Cloud Application Catalog.

Enterprises can delegate admin activities to local or regional teams whilst MSPs can reflect responsibilities within SLAs or use role based access control to enable value added services.

Different email addresses can be entered to receive notifications relating to system, maintenance, unblock and log archive notifications.

Parent accounts can assume the administrator role for a child account to manage settings, policies and rules across all services, or troubleshoot issues, on behalf of business units or customers.

EASE OF ADMINISTRATION

There is a single identity store within the Censornet Platform that is shared across Email Security, Web Security, Cloud Application Security (CASB), Identity-as-a-Service (IDaaS) and Multi-Factor Authentication (MFA).

For organizations with Microsoft® Active Directory there are options for Local Sync or Cloud Sync. Local Sync uses a locally installed AD Connector Service (agent) which pushes objects to the Censornet Cloud. Cloud sync uses a LDAP or LDAPS connection to pull objects. Local Sync has the additional benefit of not requiring any firewall rule changes. Both methods require a read only service account in AD.

For those organizations that do not have AD, local usernames will still be captured where possible.



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



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



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



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



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



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, seamlessly with identity management and advanced data loss prevention to activate the Autonomous Security Engine (ASE).

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

Advanced DLP

Prevent sensitive data getting into the wrong hands.

Enterprise-grade DLP across email, web and cloud applications for the ultimate real-time protection.

Autonomous Security Engine

Prevent attacks before they enter the kill chain.

Enable traditionally silo'd products to share and react to security events and state data whilst leveraging world class threat intelligence.

CENSORNET LTD

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

Phone: +44 (0) 845 230 9590

CENSORNET LTD

Park Allé 350D, 2605 Brøndby,
Denmark

Phone: +45 61 80 10 13

CENSORNET LTD

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

Phone: +1 (877) 302-3323