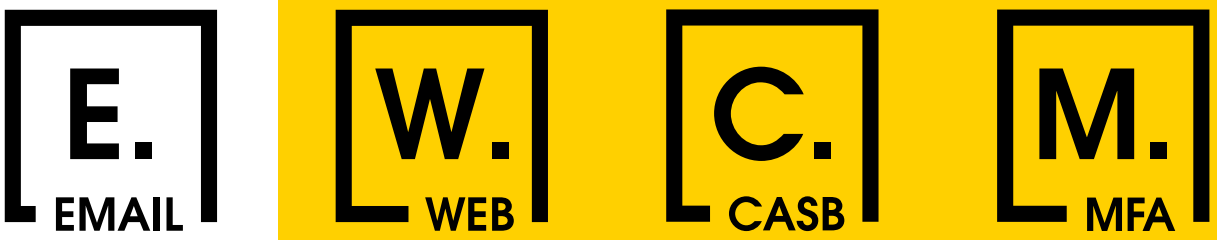
24/7 ATTACK PREVENTION & SAFEGUARDING FOR EDUCATION

censornet.

THE PLATFORM FOR COMPLETE SECURITY

Censornet's cyber security platform enables comprehensive monitoring and in-depth control of web, email and cloud application use to protect students from cyber-bullying, online radicalisation as well as inappropriate or malicious content – including viruses and other malware.



With over 10 years' experience in the education sector the Censornet platform includes numerous predefined template policies, rules and keyword dictionaries to simplify implementation and ensure rapid compliance with safeguarding guidelines.

Censornet specialise in providing true enterprise grade security at a price point accessible to schools, academies, colleges and Universities.

ONE PLATFORM, ONE PANE OF GLASS

Our world-class cyber security platform provides rich data visualization and reporting across all Censornet services and an extensive set of attributes and criteria.

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).

Reports can be linked to schedules and sent via email as CSV or PDF attachments. Scheduling can also be used to provide near real time email alerts to certain pupil actions, or the occurrence of specific keywords across email, web and cloud application use.

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 platform will provide the evidence needed.

Our cloud platform is included with the purchase of any Censornet service. Additional services can be added to the platform at any time.

INTELLIGENT WEB FILTERING

Censornet Web Security provides filtering of over 500 categories of web content covering billions of web pages. The solution includes both the Counter Terrorism Internet Referral Unit (CTIRU) (Prevent) and Internet Watch Foundation (IWF) illegal sexual content lists.

Advanced filtering enables educational establishments to comply with the UK Home Office Prevent strategy and the Counter Terrorism and Security Act 2015 and meet their duty to demonstrate "due regard to the need to prevent people from being drawn into terrorism".

- Different policies can be quickly and easily created for different ages or year groups
- Integrated with Microsoft® Active Directory for simplified user and group policies
- Simple workflow for managing access to websites and responding to unblock requests (can be actioned by teachers, faculty or year heads, not just IT staff)
- Scheduled and Time Quota access to site categories allows for more relaxed lunchtime and after-school policies
- Intelligent appropriate filtering ensures protection of pupils from harmful or inappropriate material without being overly restrictive and impacting on learning
- Specific categories cover anonymous browsing and proxy bypass sites

Censornet Web Security also includes the ability to analyse web pages in real time for keywords and phrases that are associated with discrimination, bullying, self-harm, violence, grooming, radicalization and extremism, with the convenience of pre-populated dictionaries. All dictionaries can be extended or customised if required.

Adverts within web pages can also be removed to protect young people from distracting or inappropriate brand messages, as well as malvertising which increasingly affects mainstream sites that aren't typically blocked.

SAFE SEARCH FOR SCHOOLS

Safe search can be enforced on popular internet search engines such as Google, Yahoo and Bing. Specific keywords or phrases can be blocked from being used in search strings. All searches are saved to provide an audit trail of which pupils searched for what terms or topics on the internet.

CLOUD ACCESS SECURITY – GOING BEYOND BLOCK AND ALLOW

Few websites today are entirely static. Most support a level of user interaction and are therefore applications, even if the site is a news site that simply allows users to comment on articles and stories.

Increasingly organizations need to implement granular policies that manage user actions within web applications. Simply blocking or allowing sites is no longer a viable solution that balances student protection with the need to learn.

Censornet Cloud Access Security provides visibility of all user activity within web or cloud applications, driven by an app catalogue that contains hundreds of applications and thousands of user actions. If a web application is allowed, specific features within the application can be monitored or blocked. Using simple rules, sites can be made read-only.

Keywords can be used to ensure that the content of messages, posts and tweets is appropriate and not derogatory to the organization, or staff. Files uploaded to cloud storage applications – such as Dropbox, or Microsoft® OneDrive – can be scanned for content, and malware.

ULTRAFAST AND UNOBTRUSIVE

Censornet uses a unique architecture that doesn't proxy all web traffic, ensuring an ultrafast and transparent experience that doesn't impact productivity or cause user frustration.

The Censornet Cloud is built on world-class infrastructure (including Amazon, Microsoft and IBM) in multiple locations for unparalleled speed, scalability and resilience. Personal data is regionalised to ensure local data protection and privacy requirements are met.

E.
EMAIL

EMAIL SECURITY, ARCHIVING AND CONTINUITY

Censornet offer a comprehensive set of email security services from industry-leading protection from spam, phishing and malicious attachments, to solutions for sending email securely (encrypted email messaging), to archiving all email messages inbound and outbound, to providing an emergency inbox in the event that the primary mail provider suffers an outage to ensure continuous access to sent and received messages (until service is restored).

At the core of the Censornet Email Security (EMS) service is a powerful cloud-based mail routing engine that allows email administrators to control exactly how email flows in and out of the organization. Multiple email providers can be supported, for example, so staff and students can use different email services (e.g Gmail, O365, Microsoft Exchange).

All aspects of inbound and outbound messages can be inspected – including headers, sender, recipient, subject, body, attachment type and size. Actions available include accept, reject, re-route, add content to subject/body/headers and quarantine based on message attributes and content.

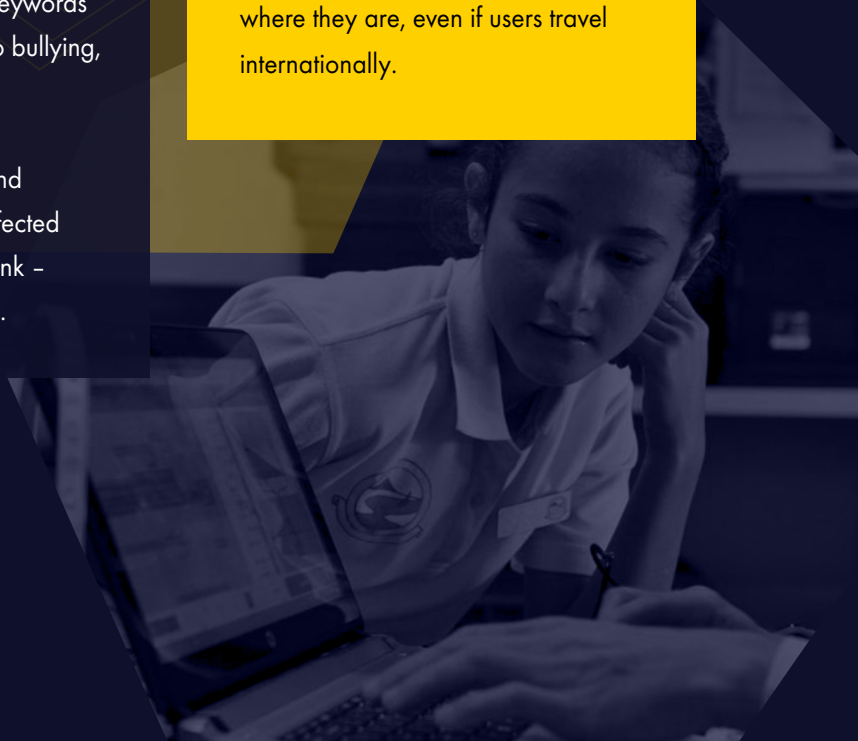
Inbound and outbound emails can be analysed for keywords and phrases with customisable dictionaries specific to bullying, sexual content and obscenities/profanities.

Censornet LinkScan rewrites all web links in emails and provides point-of-click protection from malicious or infected web pages, regardless of when a user clicks on the link – even months after a message was originally received.

PROTECTION INSIDE AND OUTSIDE THE CLASSROOM

Censornet uses a combination of gateways and agents to protect students on and off the network, regardless of the device used. Furthermore, the Censornet Cloud Gateway features a captive or guest portal to ensure rules and policies are applied when students use their own personal devices to access web-based resources inside and outside the classroom, supporting BYOD initiatives.

Agents for Windows and Mac OS X protect devices regardless of where they are, even if users travel internationally.



OUR PLATFORM

Our cloud security platform integrates email and web security, CASB (Cloud Access Security Broker) and adaptive MFA (Multi-Fator Authentication) activating the Autonomous Security Engine (ASE) to take you beyond alert driven security and into real-time automated attack prevention.

E. EMAIL

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

W. WEB

Protect users from web-borne 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.

ASE

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.

Ready to transform your security into 24x7 protection?

Visit censornet.com
or call +44 (0) 845 230 9590