CENSORNET
UNIFIED SECURITY SERVICE

CensorNet Unified Security Solution

Censornet USS enables you to monitor and control Web, Email and Cloud Application use to provide complete security for your organisation from one dashboard. You can protect your employees, whether in the office or mobile, against cyber-attacks, and accidental or malicious leaks of sensitive data. Keeping your organisation safe from from the risks associated with the rapid growth in cloud applications, and the emergence of Shadow IT.

USS is a comprehensive cyber security service that combines modules for the security, monitoring and control of web, email and cloud application across your network in one dashboard and logging service, meaning that common policies can be easily applied and incidents tracked across different media.

USS provides the security and control of an on-premise or end point component with the flexibility and mobility of a cloud service. It is the next generation in Email and Web security with Cloud Application Control giving you the power to extend web access policies to Bring Your Own Device initiatives and to monitor and control Shadow IT.

Telephone: +44 (0) 845 230 9590 . **Email:** info@censornet.com **www.censornet.com**

Cloud Application Visibility

Detect cloud application usage and activity to reveal which applications are being used from your network. Drill down into application activity by individual user, device, URL and action.

You can track files as they are moved between web applications and shared via email, social media, file sharing or other cloud applications, and an individual's activities across different devices.

It is easy to get a view of all the cloud applications being used over your network, authorised and unauthorised, who is using them and what for, even looking into the content of suspicious or risky activity.

Cloud Application Control

By downloading the CensorNet cloud link client to mobile devices or routing through the cloud gateway the use of cloud applications can be controlled.

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.

That means that someone can have access to an application that includes sensitive data as view only when they are using a tablet in an airport, but are able to download or print the same information when using their laptop at their desk and connected to the corporate network.

Safe anywhere on any device

You can set internet access policies at group or individual user levels. These policies are enforced even when users attempt to circumvent controls by using anonymising proxy sites.

Policy can be enforced, and protection from malware is in place, wherever your users access your network, whether from home or the office, on a desk PC, a laptop or tablet running the CensorNet agent, or even a smartphone connecting via the gateway, they are protected.

Safe Web Access

Over 140 categories of web content covering billions of web pages, are constantly updated for accuracy and protection.

New URLs are classified in real time to ensure only acceptable content can be accessed.

Administrators can maintain their own URL categories that can be applied to create or override exceptions within the filter policies.

You can enforce safe search mode on popular search engines such as Google, Yahoo, Bing and You Tube and restrict use of applications like Google Apps to a corporate domain, thus preventing personal use of webmail.

Fast and Unobtrusive

Uses a proxy-less approach which reduces latency and preserves the user's real IP address, as well as preserving privacy by allowing the browser to maintain direct communication with the designated website, as long as that website is approved for access by that user. This enables mobile devices with GPS to be used to access cloud applications that use location information, without causing an identity theft false alarm, or error messages for mobile employees when they are remote from the IT team.

It gives a fast and unobtrusive experience that doesn't hinder productivity or cause frustration, and extends to networks, roaming users, standalone computers, tablets and smartphones – providing complete visibility and control of who is using your network for what.

Analytics across email, web and applications

You can easily apply consistent policies regardless of the means of communication and have complete visibility of who is doing what on your network with the ability to track data as it is moved between emails, web applications, social media, and file sharing. Setting up alerts for high risk activity.

Safe from Malware

The CensorNet services scan all emails and web traffic and blocks malware before it reaches your network.

Incorporating multiple layers of security such as on-line threat detection, reputation and heuristics across multiple platforms, CensorNet uses an effective combination of tools and approaches.

Deep HTTPS inspection allows SSL encrypted content to be scanned for malware

Email Security

CensorNet Email offers a security and backup service that scans both inbound and outbound emails for malware, phishing, content violations and spam.

By doing this in the cloud it removes the processing and bandwidth burden on the local email server and also provides a layer of resilience in case of local mail server failures.

At the core of CensorNet Email Security is a sophisticated rules engine that allows the IT administrator to customise exactly how email flows in and out of the organisation. The rules engine can inspect all aspects of email, including content, attachments, size, headers, recipients to name but a few and take appropriate action, such as quarantine, re-route, notify, reject and more.