CENSORNET
USS WEB MODULE

Unified Security Solution: Web

CensorNet's USS Web Module empowers you with the best of on-premise and cloud web security, brought together in a single analytics, reporting and management portal. Add Cloud Application Control and you can safely benefit from the huge advantages that cloud applications bring while maintaining complete visibility and control.

Designed to act as an umbrella for web security across head office, branch office and remote workers, USS: Web Security provides a single pane of glass to discover, analyse and control web activity across multiple networks and devices.

Uniquely, the USS platform uses 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 designated web server if the request is allowed. This results in a fast and unobtrusive experience which does not hinder productivity or cause frustration to end users.

In addition, the follow-the-user philosophy ensures web access control passes seamlessly from desktop to laptop to mobile and therefore provides a consistent browsing experience for the end user. More sophisticated than DNS-based solutions and involving considerably less overhead than pure proxy solutions, the USS platform extends to networks, roaming users, standalone computers, tablet devices and BYOD - providing the IT department with complete visibility and control.

USS:Web Security incorporates a wide range of web access control functionality including URL reputational analysis of billions of web pages and a sophisticated policy and reporting engine. Combine it with USS : Cloud Application Control and it provides not only protection from malware delivered through cloud apps but visibility and control to prevent loss of sensitive data and the ability to enforce policies to maintain regulatory compliance.

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

www.censornet.com

Key Benefits	Key Features
Shine the Light on Shadow IT *	• Detect Cloud application usage and activity • Reveal which cloud applications are in use on your network by individual and category • Visibility of how the cloud applications, sanctioned and unapproved, are being used • Insight into content being downloaded, communicated or shared within the cloud apps
Safe Cloud Adoption *	• Control access to cloud applications by individual user, group, device, and function within the application • Control actions within a cloud application like file uploads, posting messages and storing data • Creates an audit trail of all cloud activity • USS Gateway - provides control for BYOD. USS Agent provides control for roaming users (Windows)
Proactive Web Security	• Stops web malware before it reaches your network users • Automatic unknown URL classification • Automatic anonymous proxy detection • Intelligent URL filtering • Dashboard reporting
Rapid Return on Investment	• No management hardware or software to support • Pay as you go per user/per year subscription model • No set-up fees or other up-front costs • Central management and reporting of all users across multiple deployment options, reducing administration.
Easy to Manage	• Intuitive and customisable web based management portal • Flexible deployment methods for any type of network • Active Directory Integration • Easily scalable • Real time cross protocol logging and reporting • Unique architecture provides a fast low latency service

• Requires Cloud Application Control Module

Business is changing with employees conducting business on and off the network, more business applications in the cloud, BYOD and easy access to a growing number of cloud applications for end users, all making security more complex.

CensorNet's USS recognises that a new type of solution is needed, that balances the need for security with usability, to prevent internet abuse, enforce content and access policies and protect against malware risks whatever the threat vector.

Features

SECURITY	
Real-time Anti-Malware Scanning	Incorporating multiple layers of security such as online threat detection, reputation and heuristics across multiple platforms
URL Reputation	Over 140 categories of web content cover billions of web pages in multiple languages, constantly updated for accuracy and protection. Includes Internet Watch Foundation (IWF) illegal site database.
Automatic Unknown URL Classification	New URLs are classified in real time to ensure only acceptable content can be accessed
HTTPS Inspection	Control access to SSL encrypted content. Deep HTTPS inspection allows SSL encrypted content to be scanned for malware - available on Cloud Gateway component.
Anonymous Proxy Detection	Prevent access to anonymous proxy sites
Embedded URL Scanning	Detect and block attempts to access content even if the URL is embedded deeply in the URL
Safe Search	Enforce safe search mode on popular search engines such as Google, Yahoo, Bing and YouTube
BYOD Access Control	Support BYOD by safely allowing BYOD access to the network via the built-in Captive Portal feature
URL Overrides	Administrators can maintain their own URL categories that can be applied to create overrides and exceptions within filter policies.
Cloud Application Discovery *	Detect Cloud Application usage and activity and reveal which applications are in use
Cloud Application Control *	Control access to Cloud Applications at a granular level down to the feature and actions within the application

* Requires Cloud Application Control Module

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, single-sign-on, and direct to cloud (internal)
User Synchronisation	Active Directory synchronisation service ensures changes to Active Directory are replicated. Import wizards are also available for importing users from various sources
Web User Interface	A modern, clean and rich user interface provides an easy to use administration panel
Delegated Administration	Allows creation of multiple administrators with different levels of access to the administration interface
Customised Notification Pages	Brand the notification pages (such as Access Denied, Captive Portal, etc.) with text, logo and terms of service information

REPORTING	
Real-time Visibility	Productivity charts display instant visibility on compliance with defined access policies. Query in real time web activity by user, domain, group and category. See exactly which users are browsing and drill down into activity including those users that are triggering policy violations
Report Builder	Administrators can define their own reports based on available field names and criteria. Reports can be saved and then exported to Excel
Top Trend Reports	A selection of pre-defined trend reports with chart and table data. Trend reports can be exported to Excel and e-mailed to recipients.
Cross Protocol	logging, analysis and reporting by user, group, application, device, action.

DEPLOYMENT OPTIONS	
Software for Networks	Available as a downloadable software, CensorNet's Cloud Gateway software can be deployed on a virtual server or physical server in less than 30 minutes to extend security policies to the entire network
Agent Software for Roaming Users or Standalone Devices	Microsoft Windows agent that enforces policies on the device. Tamper proof and simple to deploy either with an install wizard or scripted via Active Directory Group Policy. Mac OS X version will be available soon.
Secure Browser for iOS	A secure browser app for iOS6 and above provides an alternative to Safari which extends the web access controls to the mobile device
Scalable	Highly optimised for large networks, the solution takes advantage of multiple processors, all available RAM and has a 64-bit architecture
Deployment Modes	Agent software, Direct proxy (set by group policy, WPAD or manually), or gateway mode for guest, BYOD or non-domain devices
WPAD Support	Automatic creation of Web Proxy Automatic Discovery (WPAD) file based on network configuration
BYOD Captive Portal	The Captive Portal allows existing users or guests to adopt BYOD and log in from those devices with valid user credentials e.g. Active Directory