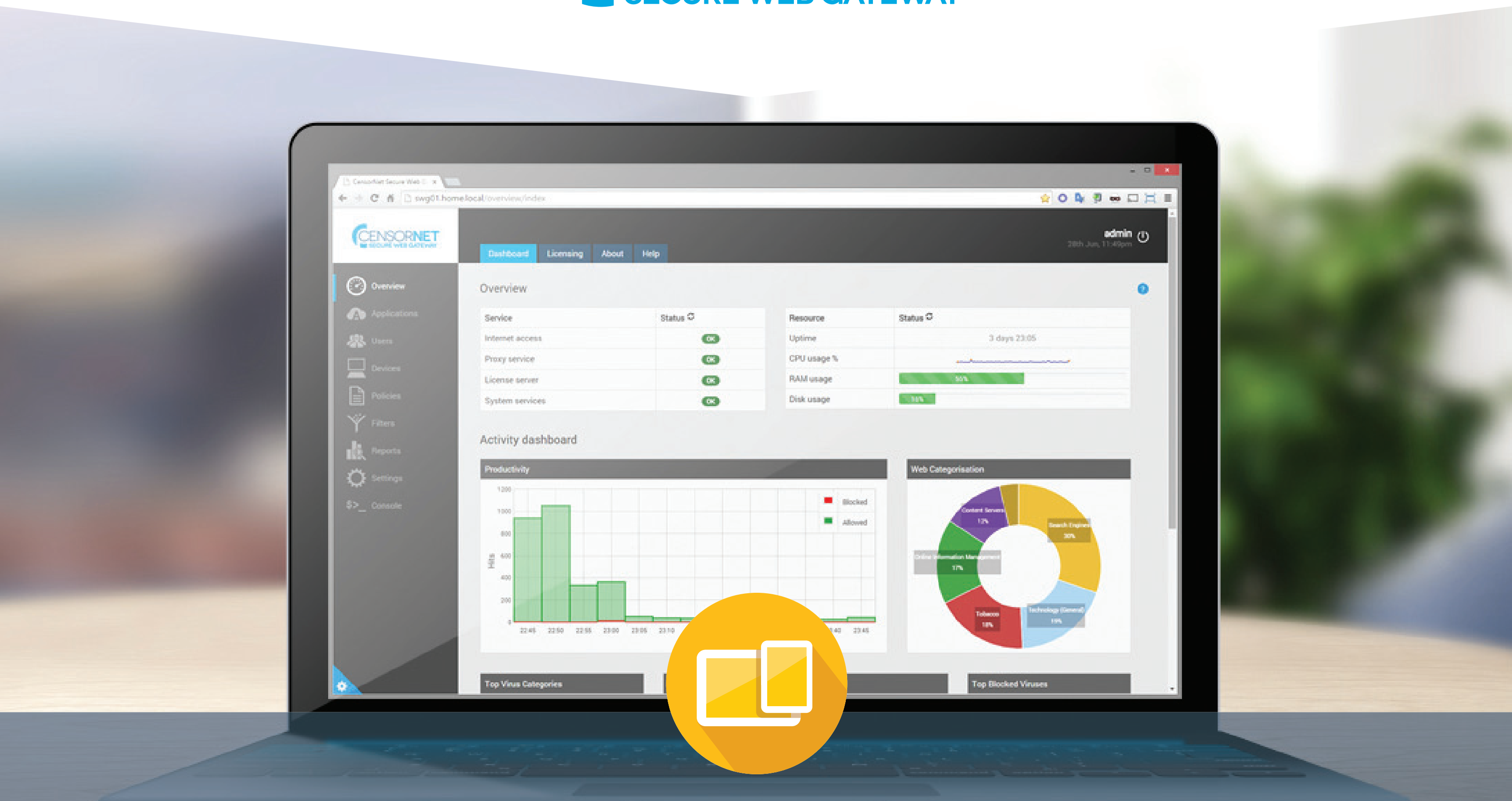
CENSORNET
SECURE WEB GATEWAY



Overview

Service	Status
Internet access	OK
Proxy service	OK
License server	OK
System services	OK

Resource	Status
Uptime	3 days 23:05
CPU usage %	
RAM usage	50%
Disk usage	15%

Secure Web Gateway

CensorNet SWG is CensorNet's next generation secure web gateway with built-in Cloud Application Control capability and the power to extend web access policies to Bring-Your-Own-Device (BYOD) initiatives.

Web access for employees is business critical and cannot be avoided. However, IT departments also face the challenge of how to accommodate trends like the rise of cloud applications and BYOD initiatives without compromising network security and bandwith. CensorNet SWG provides organisations with enterprise-class web access control, filtering and reporting whilst safely enabling the adoption of cloud applications.

The demand for cloud applications is unprecedented and the binary "allow" or "block" approach of traditional web security proxies either restricts cloud adoption or opens the flood gates to potential data breaches or misuse; in both cases having a negative impact. CensorNet SWG allows organisations to embrace the cloud application revolution by implementing discovery and analysis functionality across all devices used on the corporate network.

In addition, the solution provides a wide range of web access control functionality such as real-time anti-malware scanning, URL reputation analysis of billions of web pages, real-time image content scanning and a robust and sophisticated policy and reporting engine.

Key Features

Security - provides robust web security and cloud application control capabilities including malware and web-borne threat protection, URL reputation and image scanning technology. Light or deep SSL scanning included as standard.

Management - provides a flexible policy engine, time and quota setting by user or device group and includes authentication, cloud application discovery and easy BYOD adoption.

Reporting - Offers real-time reporting including visibility of productivity and compliance by user, domain and actions, cloud application analysis, top trends and bandwidth as well as a customised report builder.

Deployment - The software can be deployed on a virtual server or physical server and is optimised for the most demanding networks.

Key Benefits

Increase network security - prevents accidental or intentional access to malware, inappropriate and illegal web-based content using the latest real-time scanning technology from BitDefender.

Shine the light on Shadow IT - discover in real-time what cloud applications are in use across a broad spectrum of services, from Cloud Storage and CRM to E-mail and Social Networking.

Safe cloud application adoption - embrace cloud applications safe in the knowledge that actions within them, such as file uploads, posting messages and storing data, can be made visible and risk attributed.

Enable BYOD - allows employees to use their own devices and extends their web access policy to those devices for a consistent web-browsing experience.

Increase productivity - embraces cloud applications, BYOD initiatives and limits access to time wasting websites during working hours.

Improve bandwidth availability - blocks or restricts access to bandwidth intensive downloads or applications.

Achieve compliance - helps compliance with BECTA , CIPA and other regulatory compliance related to web activity.

Rapid return on investment - prevents malware outbreak and associated down-time and costs which delivers instant return on investment.

Low total cost of ownership - a simple licensing model based on actual usage, easy deployment and no hardware or 3rd party software licensing requirements.

Reduce legal risk exposure - blocks known illegal content, inappropriate images and web content and creates an audit trail of activity for every user on the network should evidence be required.

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.
Image Analysis	Images are scanned for inappropriate adult content and are replaced with safe symbols before being displayed in the web browser.
Cloud Application Discovery	Detect Cloud Application usage and activity within known applications and reveal which applications are in use on your network.
Automatic Unknown URL Classification	New URLs are classified in real-time to ensure only acceptable content can be accessed.
HTTPS Inspection	Deep HTTPS inspection allows SSL encrypted content to be scanned for malware and hidden threats removed.
Anonymous Proxy Detection	Prevent access to anonymous proxy sites.
Safe Search	Enforce safe search mode on popular search engines such as Google, Yahoo, Bing and YouTube.
YouTube for Schools	Turn YouTube into an education friendly resource with support for YouTube for Schools.
File/MIME Scanning	Block file types and MIME types to prevent downloads and streaming media saturating network bandwidth.
BYOD Access Control	Support BYOD by safely allowing 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. Domains can be by-passed for authentication, SSL interception or entirely, if no filtering is required.
MANAGEMENT	
Policy Engine	Flexible policy engine allows policies to be applied to user groups or device groups.
Filter Modes	The policy engine supports 5 filter modes including filtered (granular rules), unfiltered, restricted (walled garden), blocked and advisory (coaching mode).
Time Schedule	Policies can be applied on a rolling 7-day time schedule.
Time Quota	Time based quotas can be applied to policies, for example, access to social media sites can be allowed for 1 hour per day during working hours.
User Authentication	Multiple authentication methods are supported including Active Directory single-sign-on, Active Directory prompted, LDAP, internal and none.
Device Identification	Devices can be identified by MAC address, IP address or hostname.
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 responsive user interface provides an easy to use administration interface.
Delegated Administration	Allows creation of multiple administrators with different levels of access to the administration interface.
Unblock Request Management	Integrated feedback loop between end users and the administrator for streamlining requests to unblock web content.
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, device, domain, action. See exactly which users are browsing and drill down into activity including those users that are triggering policy violations.
Cloud Application Analysis	Detailed dashboard revealing Cloud Application usage on the network. Instantly see top users, top applications, classes of applications and usage over time. Drill down into application activity by user, device, URL and action.
Report Builder	Administrators can define their own reports based on available field names and criteria. Reports can be saved and run with dynamic options and then exported to Excel.
Top Trend Reports	A selection of 20 pre-defined trend reports with chart and table data. Trend reports can be exported to PDF and emailed to recipients.
Bandwidth Reports	Report on bandwidth usage by user, device, group, domain and category.
DEPLOYMENT	
Software	Available as a downloadable software CensorNet Professional can be deployed on a virtual server or physical server in less than 30 minutes.
Scalable	Highly optimised for large networks, the solution takes advantage of multiple processors, all available RAM and has a 64-bit architecture.
Deployment Mode	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 to adopt BYOD and log in from those devices with valid user credentials e.g. Active Directory.
Multiple Networks	Multiple physical networks or VLAN's can be configured by adding additional network interfaces to the software appliance.