Web Security with Real-Time Web Content Filtering & Security

In partnership with Censornet

Prepared by Platinum Partner: CM Security Ltd

Dalton House
Windsor Ave
London SW192RR
2016
Index:

1. Management Summary
2. CM Security Ltd
3. Censornet Overview
4. CensorNet product features
5. The Cloud Gateway – what it is and its role in a hybrid option
6. Checklist of unique benefits
7. Managed Cloud Services – Inclusive services with no quibble guarantees
8. Resources
9. Protection & Security
10. AD Integration
11. Some clients
1. Management Summary

This document has been prepared to give an overview of a hybrid cloud hosted web filtering service available to valued customers who do not want to buy and regularly refresh hardware and who want to relieve valuable technical staff from supporting another system (device) on their network, without spending hours supporting it and who want their web security protected secure and fast without loss of performance to users.

The hybrid web security Cloud hosted service is fully protected and designed to remove any latency when accessing the Internet. The Cloud service is not a Proxy. It enables and empowers users to access the Internet from literally any world breakout and data is secure uncomplicated and moving fast without VPN architecture.

CM Security Ltd partners a number of appliance based web and email filtering vendors, some of whom form the basis of our own cloud managed services (IaaS), matched with qualified and highly certified Microsoft Engineers who have the skills to successfully integrate the system with any network platform. CM Security Ltd offers a beginning to end project management service that includes a security risk assessment, best practice advice and independent recommendation of fitness for purpose to ensure that all network devices work with each other.

In the best interests of mixing a system that can accommodate a high bandwidth overhead, the Hybrid Web Security from CensorNet is much more than the restrictive Proxy in a Data Centre. Furthermore speed of deployment of CensorNet is superior to any of the web security system providers.

2. CM Security Ltd.

CM Security Ltd offers Cloud services and managed services in Web Security and Protection as well as hosted network applications with its partner companies and operates from a number of data centres in UK. Its data centres serve clients in Financial Services, Property, On-line retailing, Travel, Banking, Insurance, and specially regulated businesses. We have a large number of schools and colleges who benefit from our cloud hosted systems and currently serve over 30,000 users in different sectors of industry, in different types of networks with different types of applications, products and services.

CM Security Ltd is a platinum partner with different vendors ranging from on estate system appliances to Hosted Cloud services as an MSP to out-sourced IT Consultancy and Support. CM Security Ltd and its staff have been working in companies in Security and Protection for more than 15 years. We provide the conduit between Security Vendors and integration of the right kind of Security and Protection architecture. This comes from years of experience in Corporate Networking in Client Server and Thin Client Platforms. CM Security offers a wide range of additional services including network design, build and support and specialises in security solutions that integrate with all types of networks. CM Security Ltd partners Pulsant, to provide an always on Cloud web and email filtering Service, a Cloud Application service that is built with clustered resources (2012 Hyper V cluster). CensorNet, who themselves globally partner IBM Softlayer have made their global resources available to CM Security Ltd who offer this unique cloud hosted service that is unrivalled in the web security market.
3. CensorNet – Overview

CensorNet was formed in 2007 with the organization based in Bristol Science Park, (R & D Centre) and Basingstoke UK. Its research and development takes place in Bristol which is recognized as a key entrepreneurial technology hub here in the UK. The two founding members, Tim Lloyd and Dan Searle both passionate technologists formed CensorNet to develop class leading web and email filtering products. Having built an extremely talented development team they launched their initial product in 2009 and since that time have attracted over 600+ long term customers who came to CensorNet purely based on recommendation and referrals by existing customers within the Network Security community. Somewhat uniquely there were no Sales or Marketing involvement in building this customer base.

In November, 2014 CensorNet, the next generation cloud security company, was acquired in a deal secured by a group of industry veterans, led by the new CEO and chairman, Ed Macnair who has spent 25 years in the Network Security sector. The acquisition and investment has enabled CensorNet to accelerate product development, which includes a new cloud security offering which is aligned to the growing market need for cloud based and applications and data.

Macnair and his new board of directors, Dr Steve Garnett, Craig Probert and Tim Cagle, bring a wealth of relevant industry experience and funding to the business with proven track records in successfully developing and leading technology organisations.

Macnair was founder and CEO of SaaS ID, a UK based single-sign on and application security vendor, which was acquired by Intermedia Inc. in September 2013. Before this, he was CEO of Marshal, a global web and email security company which merged with US based web security provider 8e6 Technologies to form M86 Security. Macnair has also held senior management positions with MessageLabs, Symantec, IBM and Xerox.

Ed Macnair, CEO and chairman of CensorNet, comments: The internet has changed the way we do business, but security technology has not caught up with the increased use of cloud applications in the workplace (source Gartner).

“Organisations demand greater visibility to understand and manage the security risks posed by users’ accessing the web and cloud applications. Today’s cloud security solutions need to be able to provide in-depth discovery capabilities and detailed analytics around internet and web application usage as well as providing robust security to protect against web-borne threats. CensorNet is well-positioned to help organisations address these challenges and we are passionate about the opportunity to bring this exciting technology to a wider market.”

CensorNet helps organisations step up to the challenge of managing an increasingly mobile work environment. Its solutions give greater visibility to senior management and much better control to IT over company-wide internet access and the use of web applications across all devices, regardless of whether users are in-office or mobile. It gives organisations the power to address productivity, security and audit issues associated with the growing use of mobile devices and helps them safely implement BYOD (bring your own device) initiatives into the business.
4. CensorNet product features

CensorNet’s Hybrid Web Security (HWS) 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 assuming the user request has the security rights that allows it. This results in a fast and unobtrusive experience which does not hinder productivity or cause frustration to end users.

CensorNet HWS incorporates a wide range of web access control functionality such as real-time anti-malware scanning, URL reputation analysis of billions of web pages, multi-platform endpoint software and a sophisticated policy and reporting engine. 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 safe search mode can be enforced 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.

CensorNet’s HWS has been designed to provide a consistent web access experience across multiple devices and networks – without proxy-ing between the customer network or the endpoint and the cloud service. The easy to use yet powerful web dashboard provides a single UI for web activity across your organisation. The following diagram illustrates the components of the system:

Cloud Link for Windows –is a software agent that runs on 32-bit and 64-bit Windows operating systems. Cloud Link intercepts web traffic on any web browser and provides transparent
authentication with Active Directory. The service is secured with a password to prevent the end-user from disabling or uninstalling it.

Cloud Link for iOS – this is an app for Apple iOS devices (iPhone, iPad) that provides a custom browser which can be locked down by MDM profiles

Cloud Gateway – this is a software appliance that can be installed on the network as a physical or virtual appliance. Cloud Gateway intercepts local network web traffic, provides Active Directory authentication and a Captive Portal for Bring Your Own Device environments.

5. **CensorNet Cloud Gateway**

![Diagram](image)

Deployment of cloud gateways, at each breakout for high availability is a recommended and versatile way to create the flexibility for users on the move or out of the office. The endpoints at each location can route transparently through or will proxy to the cloud gateway which manages user authentication and policy application from the cloud. It also provides a central exit point on the network for all web traffic. Any roaming devices such as laptops or company tablets/smartphones will require cloud link agents.

6. **CensorNet Hybrid Web Security checklist of benefits**

- Ease of deployment and maintenance
- Provisioning the ability to build an Acceptable User Policy for your staff across the organization by implementing and enforcing IT policies and controls
- Policy based access with users authenticated via Active Directory
- The ability to leverage the productivity benefits of securely allowing staff members to utilize BYOD (Bring Your Own Device) On-premise control of local network with Cloud Management
- On and off premises protection against malware. Real-time anti-malware scanning, URL reputation analysis of billions of web pages, multi-platform endpoint software and a sophisticated policy and reporting engine. Deep HTTPS inspection allows SSL encrypted content to be scanned for malware
- No on-premise hardware required
- No proxy required
  - which reduces latency often seen with Proxy solutions
preserves the user’s real IP address, preserves privacy because a user browser has direct communication with the designated website, as long as that website is approved for access by that user

- Centralized dashboard & Management of all users and devices

- A system that enables adherence to your businesses Compliance and Audit requirements
- Proxy-less approach provides positive, consistent user experience due to low latency. A proxy-less approach that too enables cloud delivery but mitigates importance of HA resourcing at the Data Centres
- Efficient use of network bandwidth
- Scalable & cost effective

Unified Security Solution (USS) platform is being released in late February 2016. It is the security and control of an on premise or endpoint component, together with the flexibility and mobility of a centralised cloud service.

CensorNet USS enables monitoring and control of Web, Email and Cloud Application use, and provide complete security for your organisation using one dashboard. This means protection of an increasingly mobile workforce against the security risks resulting from increasing cyber-attacks, the rapid growth in cloud applications, and the emergence of Shadow IT.
USS can allow easily applied common policies and track incidents across different media

7. **Managed Cloud Services**

Our managed cloud service is customised to fit the needs of our clients. Services are made available via the Internet, by phone and by email. Site visits are also made on request. CM Security Ltd will provide 1st, 2nd and 3rd line support. Any incident should be raised by email or telephone to our service desk where a support ticket will be open and a case reference number generated. We aim to resolve all support tickets within a 4 hour window. Our service desk is open Monday to Friday 08.00 – 18.00

Where an incident requires development intervention CM Security Ltd will liaise with the vendor to implement an effective solution.

Our managed cloud service is designed to provide easy scalable access whatever changes Companies want to make. All our cloud services are dynamically scaled to meet the needs of our users and they are refreshed regularly, managed constantly. Service level is immediate acknowledgement of ticket logging and 2 hour response although we reserve the right to respond quicker and in many cases it’s less than 20 minutes, where the nature of the request has caused downtime for users. The services provided although not confined to the list are typically:

- Service requests for support (ticket driven) such as failure to authenticate, releasing blocked pages on authorised request, Reporting – completing on demand requests for reports or production of report analysis, real time monitor management
- Execution of on demand requests from our clients’ help desk to create and manage white lists/blacklists, site categorisation, general handling of the potential of the system and management of security groups
- Site rating where appropriate (interrogation of Anonymous Proxies for examples) and management help with exceptions, Access Control Lists and general security guidance, based on 10 years of work in the industry

CensorNet allows you to control the security aspects of internet access – either blocking inappropriate sites, warning before allowing sites and logging internet activity. This provides the ability to control or monitor activity on a per user or group basis giving you complete visibility and peace of mind.

**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.

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 the network, authorised and unauthorised, who is using them and what for, even looking into the content of suspicious or risky activity. These analytics across email web and applications make it easier to apply consistent policies regardless of the means of communication.
CensorNet internet filtering software will improve your employees efficiency by allowing visibility of Cloud based applications at a granular level and at the same time reduce business risk by ensuring the ever growing demands of Compliance are met.

Not only will it improve security but also reduce bandwidth usage and provide optimal performance in organisations which have numerous offices regionally or internationally as a result of our contemporary software architecture.

Typically clients like Hassenbrook Academy use the CensorNet technology to apply an Acceptable User Policy (AUP) within the organization, complying with all business and HR requirements while still leveraging all of the productivity benefits of the ever increasing trend towards cloud based applications and data.

CensorNet also allows these AUP’s to be applied to the rapidly growing trend of staff who bring their own devices into the workplace to access corporate data irrespective of their geographical location. CensorNet’s web security products allows you to provide a safe Internet experience for all employees whether permanent or temporary within your organization enabling you to control all aspects of web access quickly and effectively.

CensorNet is a global brand and not just Europe with customers in the USA, Middle East, South America, Asia and Australia.

8. Cloud resources at the Data centre

The primary Data Centre is managed by IBM Softlayer. The UK cloud node is all hosted on IBM SoftLayer, primarily at their London DC with a satellite node in their Amsterdam DC. 
http://www.softlayer.com/network
All SoftLayer data centers maintain multiple power feeds, fiber links, dedicated generators, and battery backup. They are built from industry-leading hardware and equipment, ensuring the highest level of performance, reliability, and interoperability. With regards to compliance/standards SoftLayer are fully ISO 27001 compliant (latest standard, ISO/IEC 27001:2013) in every assessed data Centre. ISO 27001 is a widely-adopted global security standard that outlines the requirements for information security management systems

SoftLayer also provides SOC 1, SOC 2 and SOC 3 (Service Organization Control) reports on request. These reports evaluate SoftLayer’s operational controls with respect to criteria set by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles

The topology inside the SoftLayer network, works as shown below:

In addition to our Proxy-less cloud service we also operate two datacentres that host our IaaS hosted cloud service. These are in Maidenhead Berkshire and in Epsom Surrey.

9. Protection & Security

CensorNet’s HWS provides real time Anti Malware Scanning. Incorporating multilayer security such as online threat detection, reputation and heuristics across multiple platforms. Over 140 categories of web content cover, billions of web pages in multiple languages constantly updated for accuracy and protection. CensorNet’s HWS includes the Internet Watch Foundation illegal site data base. New URL’s are classified in real time to ensure only acceptable content can be accessed. Control access to SSL encrypted content. Deep HTTPS inspection allows SSL encrypted content to be scanned for malware.
Also included is Full BYOD support by safely allowing BYOD access to the network via the built in Captive Portal feature.

Administrator can maintain their own URL categories that can be applied to create overrides and exceptions within filter policies

Anti-Virus scanning provider by Bit Defender and Sophos

10. AD Integration

Full integration with Active Directory is available and often the defacto set up in order that users authenticate seamlessly and to ensure accurate usage and trend reporting. Setup (which includes an admin account for selected users to access the web filtering portal) can solicit for as many Domains as known and each AD will require a Cloud Gateway

Active Directory Integration is the best form of setup and operation giving the best form of management. It is the slickest platform to manage reporting and security management and fully supported as part of the managed service
11. Some of our clients: