WEBHAWK

CLOUD

Evaluation Guide

Powerful & Immediate Business Web Security via the Cloud

WEBHAWK
CLOUD

Contents

IMPORTANT NOTICE: All IP addresses indicated in this document are for example purpose only. Tangent support to provide the DNS IP address up on installation.

1. Introduction

Welcome to the WebHawk Cloud Service reviewer's guide. This document provides a review of the core features of the service, highlighting its effectiveness and ease of use. After reading the guide, you will have a deeper understanding of how WebHawk Cloud delivers the security you need to protect your business from the consequences of inappropriate Web use.

The WebHawk Cloud Service is part of the WebHawk award-winning security suite of products and is purpose-built for businesses regardless of sector or size. Managing Security can be daunting whether you have 30 employees or 3000. WebHawk Cloud makes implementing a web filtering solution in your company simple. Now you can enforce user browsing policies on mobile devices and gain browser policy control over nomadic workers using devices outside of the company network

Product highlights

⦿ Cloud based, so no local software installation.

⦿ Simple and quick set up: 5 minutes to get up and running.

⦿ DNS based filtering so NO latency issues.

⦿ 53 website categories to choose from.

⦿ Includes web based application filtering.

⦿ White and Blacklists.

⦿ Cloud Keys (TM) to provide customizable end user permissions.

⦿ Real time organizational browsing view.

⦿ Comprehensive on demand and scheduled reporting options.

⦿ Provides protection across multiple site and all Internet-connected devices.

⦿ Infinitely scalable and always available.
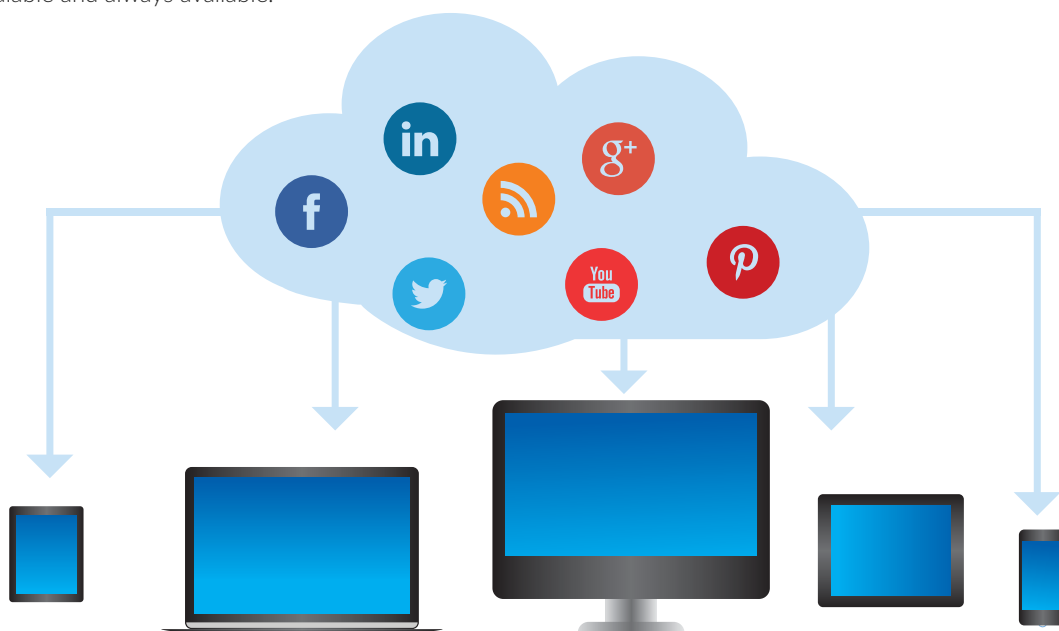
2. Set-Up & Configuration

Steps to Test WebHawk Cloud

Getting up and running on WebHawk Cloud is very simple. Here are the steps to take:

1. Send us your external IP address information

2. We will send you log on information to allow you log on and create your WebHawk Cloud Policy

3. Redirect your DNS to the IP address of WebHawk Cloud

Support can also be accessed by email at support@tangent.com

1. What we need from you
Before we can send you your unique log in details we will require you to send us all the relevant external IP addresses. This is the IP address that we will accept DNS requests from for your organization, typically allocated to you by your ISP.

2. Log on to WebHawk Cloud
We will email you a user name and password to allow you log on to your WebHawk Cloud Management interface. Here you can create you internet usage policy, create whiltelists, blacklists and reports for your organization.

3. Redirect your DNS
To set this service up all you need to do is configure your DNS server to send its resolution requests to the IP address of WebHawk Cloud. Our service utilizes two WebHawk Cloud locations, so we recommend you configure your DNS to use both, a primary and secondary in the event the primary in not reachable.

Configuring WebHawkCloud
Configuring your organization to use WebHawk Cloud can be accomplished in a number of ways.
* If your organization has an internal DNS server then you will typically either use Active Directory or Bind

Option 1 - Active Directory network
    a) Open you DNS Manager on the primary DNS server. This is usually found under Start --> Administrative Tools --> DNS.

    b) Select properties of the DNS server. i.e. click the server, then right click and choose Properties.

    c) In the Properties window click on the Forwarders tab, then click Edit, and enter the WebHawk Cloud IP addresses:

        ◉ Primary 96.127.173.70

        ◉ Secondary 173.236.14.29

OR

Option 2 - BIND

       a) Edit the bind configuration file (usually /etc/namedb/named.conf) and look for the options

            statement: options

            ...

            ...

            };

       b) Inside the options statement, you need to add a forwarders statement listing the WebHawk Cloud server(s). If a forwarders statement already exists, then edit it appropriately to point to the WebHawk Cloud server(s): options {...forwarders {96.127.173.70; 173.236.14.29};};

       c) Restart the bind service to reload the configuration.

* If your organization does not have an internal DNS server

The WebHawk Cloud IP address (es) may be configured on your router to ensure that all computers and devices that connect to that router can avail of the WebHawk Cloud web content filtering and protection.

The place to change your DNS settings on your router can vary from router to router. In general, you need to perform the following:

       a) Go to the management interface for your router (e.g. http://192.168.0.1) and enter your administrative username and password.

       b) Find the section to manage the DNS settings

       c) Replace the existing settings with those for WebHawk Cloud and save.

            ◉ 96.127.173.70

            ◉ 173.236.14.29

To ensure your new DNS settings take immediate effect, you may need to flush your DNS resolver cache and your web browser caches.

Setting your Policies

You are now ready to create your WebHawk Cloud policy. The policy tab is where you decide how to define work and non work times, what categories of websites you want to block and allow. The process is very simple with the use of on/off radio buttons. You can also now set up notifications if you wish, for example manager x is notified if access to pornography site is attempted.

Cloud Keys and HTTPS

WebHawk Cloud uses a feature called "Cloud Keys" to allow you to give an individual in the organization access to a particular website that would otherwise be blocked due to access to a URL category being blocked within your policy. This is operated with a system of Cloud Keys where by a Key is created for that user to allow them override to the blocked category.

In the current version if a user uses a Cloud Key to try and access an otherwise blocked site, where the site in question is HTTPS, they will not be able to access the site and will receive a "Cannot connect" or "Not accessible" message from the browser. The issue can be overcome using the whitelist feature whereby the domain in question can be whitelisted. So, for example, if under the policy you create, the category "Web based Mail" is blocked, and you wish to allow a user access to Gmail, as Gmail uses HTTPS, the Cloud Key system will not permit access to Gmail, so as an alternative we can whitelist Gmail.

3. Managing your WebHawk Cloud Service

a) Management console and dashboard

When you set up and configure WebHawk Cloud you will be presented with a dashboard similar to the one below:
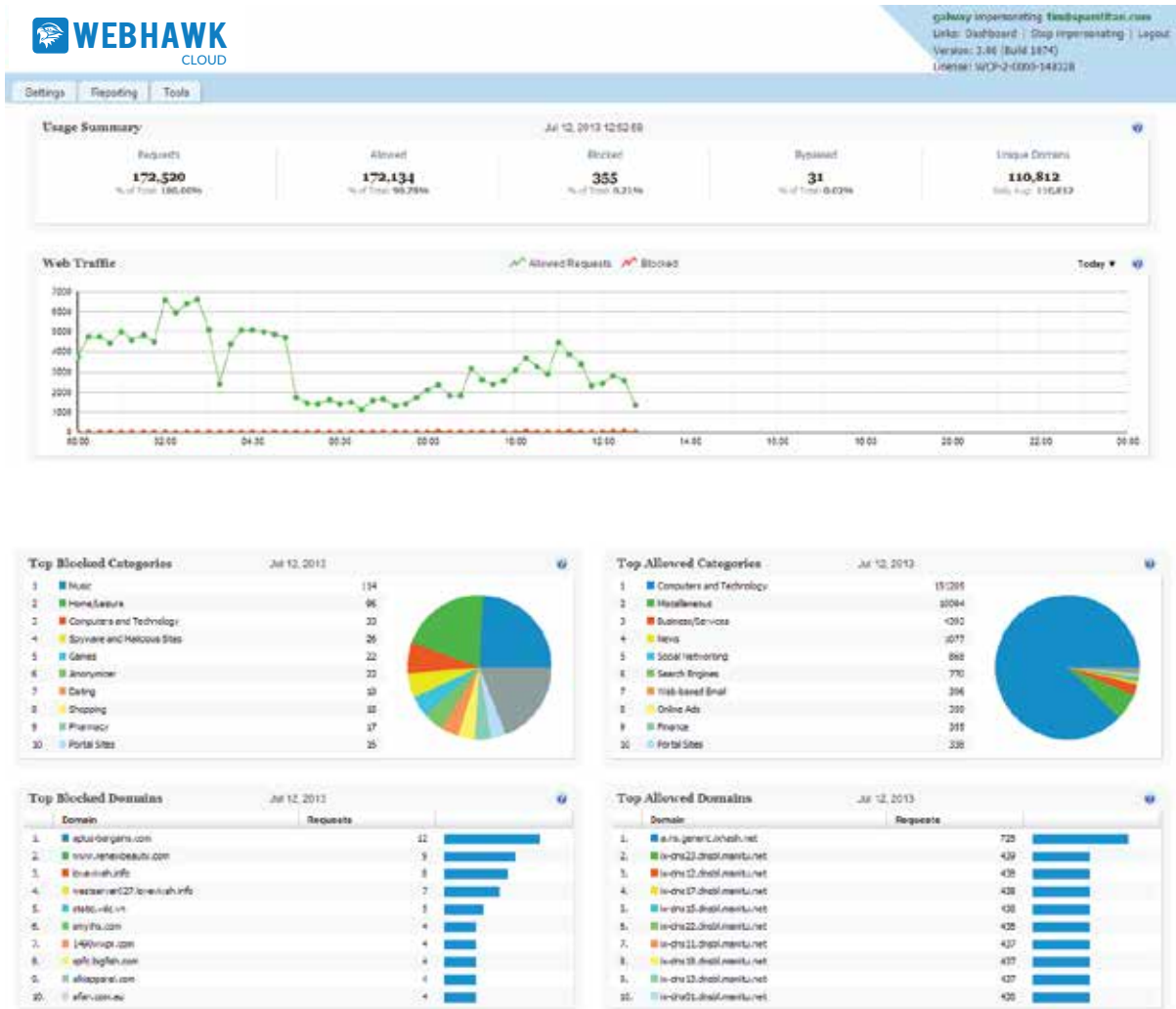
The dashboard presents a summary of web usage including number of requests, allowed requests, blocked requests and details of traffic through WebHawk Cloud together with details of top categories and domains blocked and allowed.

4. Reporting

WebHawk Cloud allows you to run reports with actionable data to change browsing policies via the WebHawk Dashboard.
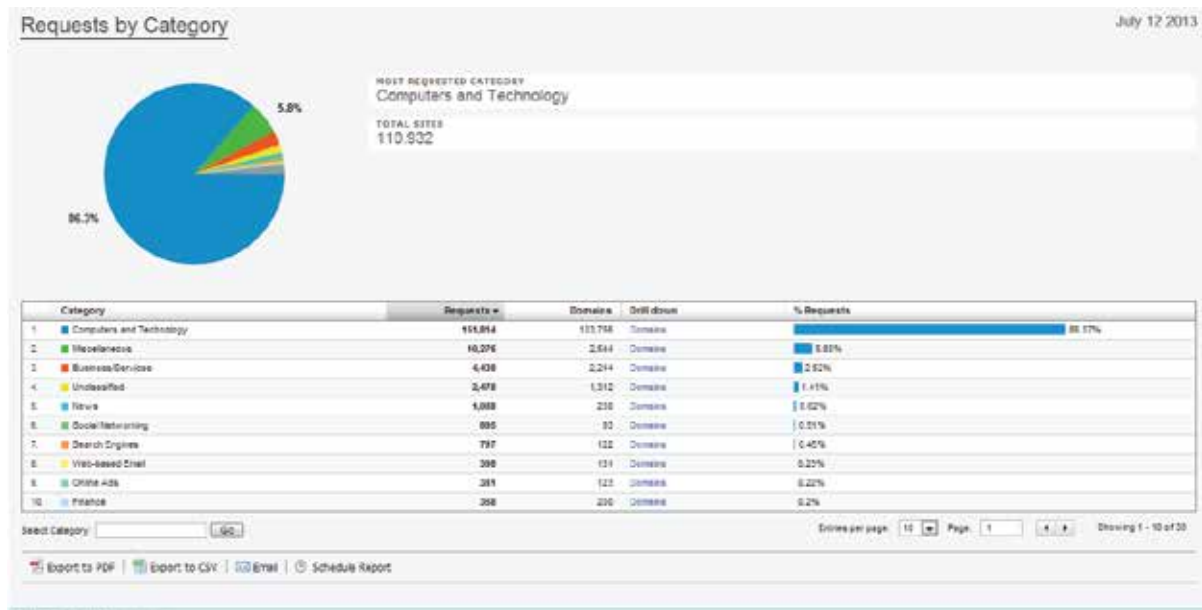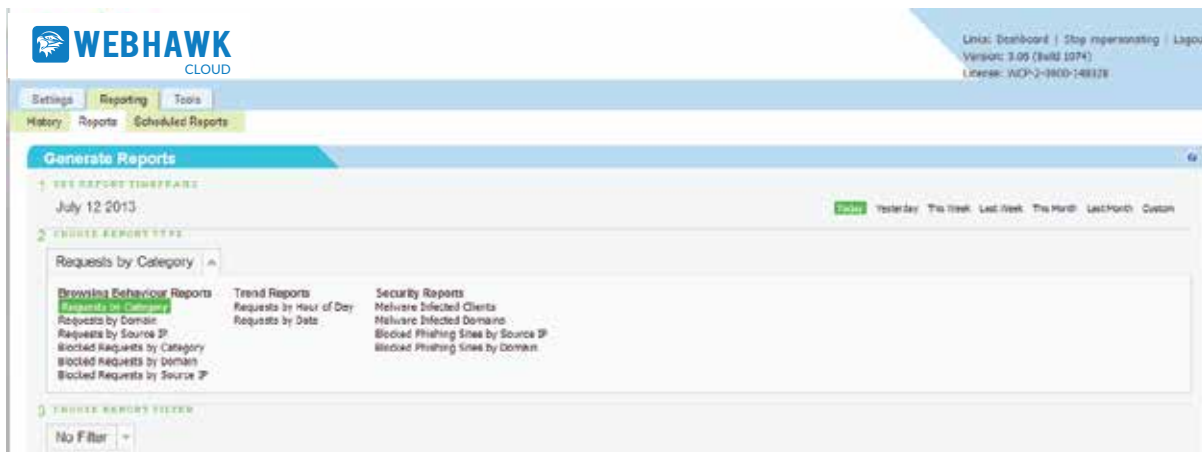
The reports module provides predefined editable reports covering all aspects of web usage including 'Request by Domain', 'Browsing behaviour report', 'Blocked request by category' and many more. All reports are fully editable allowing the user retrieve the data that is most important to them and their organisation.

5. Contact

For Technical Support, please call 800.342.9388 ext 1, or email support@tangent.com

For Sales, please call 800.342.9388 ext 2, or email 1sales1@tangent.com

For online support, please visit www.tangent.com