



Openwave Web Security

Securing the Mobile Internet

Today people own and use a wide variety of mobile devices that contain growing amounts of unsecured personal data.

In particular, sophisticated smartphones increasingly are the primary repository of important personal data. With the advent of commercially exploitive mobile viruses, mobile service providers must protect networks, mobile subscribers, and subscribers' mobile devices.

Openwave Web Security provides a comprehensive set of security options the service provider can combine to fulfill specific security needs and protect subscribers.

Subscribers want the assurance of safe internet access—for themselves and their minor children. Service providers are empowered to control minors' access to sites and content while responding rapidly to the real threat of smartphone viruses. And both service providers and subscribers want the highest level of user experience as they launch and experience exciting, new services.

Service Provider Benefits

- **Network and Subscriber Protection:** With Openwave Web Security, service providers enjoy the necessary security layers to protect their network and subscribers from inappropriate, unwanted, harmful and commercially exploitive content.
- **Rapid Deployment of Security Applications:** The Openwave Web Security architecture is based on

a plug-in framework that allows additional security applications to be quickly added as new mobile security threats emerge (Figure 1).

- **A High-Quality, Secure User Experience:** By implementing multiple defenses against unwanted content, service providers can deliver a high-quality user experience while confidently launching new and innovative services.

Subscriber Benefits

Safe Access: Subscribers benefit by safely accessing the Internet from their mobile devices. The in-network, anti-virus solution captures and removes viruses before they reach the user's device.

Control and Choice: Openwave Web Security's content control service ensures that minors are protected from accessing inappropriate content, while providing adults with the choice of accessing such content.

Features

Openwave Web Security is just one of Openwave's web enhancing services. All data traffic routed through the Openwave Context Aware Mediation Platform can benefit from these services.

In addition, the intelligent workflow engine ensures that the service provider has full control over how and when a service is invoked and also that the features of the Openwave Web Security service are utilized in an optimized manner.

Transaction Analysis:

Adult content control is applied on a per-subscriber basis by assigning an appropriate plan based on the age group of the subscriber. Minors can be assigned a "child's plan," while adults can be assigned an "adult's plan." Plans can contain one or more 'allowed' and/or 'denied' content categories.

Content requested by a subscriber who has been assigned an Openwave Web Security plan is subjected to access control. The requested URL is first checked against the Internet Watch Foundation blacklist, which contains lists

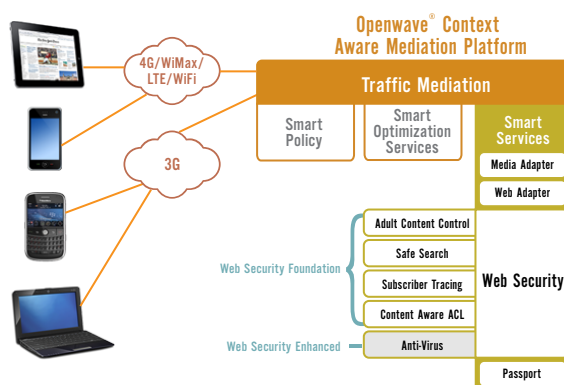


Figure 1: Openwave Web Security is a web enhancement service available on Openwave's Context Aware Mediation Platform

Openwave Web Security

of illegal sites to which all access is barred, and, if this stage is passed, the URL is then categorized using the URL FilterDB database.

If the content is categorized as “adult,” and the subscriber requesting the content has a child plan, this categorization results in the content being blocked and an appropriate message displayed. An adult accessing the same content might be allowed direct access or may be informed of the nature of the content and given the option to proceed (Figures 2 and 3).



Figure 2: Guardian blocks adult content from minors.



Figure 3: Guardian gives adults the option to view restricted content.

- Safety catch is part of Openwave Web Security’s adult content control solution. If a minor tries to search through Google or other popular search engines, Openwave Web Security will ensure that the search engine’s “safe search” option is enabled.
- Content-type access control allows the service provider to control access to specified content types from a list of approved sites. For example, ringtones might be downloaded only from the service provider’s portal or from authorized partner sites.
- Anti-virus allows selective or plan-based anti-virus detection upon request and on response paths.

Activity Monitoring

- Subscriber tracing logs the activity of individual subscribers. These logs can be accessed by customer care and can be made available to parents to check on the activities of their children or to authorities in cases of suspected criminal activity.
- Adaptive logging automatically logs activity. When a user triggers a preconfigured suspicious activity threshold (for example, repeated attempts to access

illegal content), future activities can be automatically logged for monitoring purposes.

Advanced Routing

- Redirection to a splash page offers the service provider a high degree of flexibility when deciding how to communicate to subscribers following a security-related interception. In a case where Openwave Web Security detects that an adult user is requesting adult content, the service provider can allow direct access transparently, configuring a splash page to be presented that informs the user about the nature of the content along with a choice to continue or abort.
- Another option the adult user might be offered is access, subject to first signing up to a subscription service using Passport — Openwave’s web enhancing service discovery service. A minor accessing the same content might, however, simply be informed that access is denied and provided the option of returning to the service provider’s portal to continue browsing.

Device and User Protection

- Openwave partners with a premium supplier of anti-virus software to protect valuable mobile devices and also provide safe mobile access to the Internet

Licensing Options

Since each service provider has different security needs, Openwave Web Security comes with two licensing options, each with a related feature set.

1) Openwave Web Security Foundation offers the following features:

- Adult content control leveraging static URL categorization (Internet Watch Foundation-compliant) and safety catch features.
- Content type-based access control
- Subscriber tracing
- Advanced routing/redirection to a splash page

2) Openwave Web Security Enhanced provides an optional security add-on that uses the McAfee anti-virus database. This add-on is separately licensed.

About Openwave

Openwave Systems Inc. (Nasdaq: OPVV) is a global software innovator delivering context-aware mediation and messaging solutions that enable communication service providers and the broader ecosystem to create and deliver smarter services.

Building on our mobile data heritage, Openwave mobilizes the internet with predictive solutions based on real-time analytics that mediate among all the different ecosystem elements and enhance every mode of IP traffic. The result is a 360-degree view of users, the network, devices and services that enable our customers to proactively optimize network resources, launch smart mobile services quickly, and provide a contextually relevant user experience. Openwave is a global company with a blue chip customer base spanning North America, Latin America, Australia and New Zealand, Asia, Africa, Europe, and the Middle East. Openwave is headquartered in Redwood City, California. For more information please visit www.openwave.com.

Openwave and the Openwave logo are registered trademarks of Openwave Systems Inc. in various jurisdictions. All other trademarks are the properties of their respective owners.

Copyright © 2010 Openwave Systems Inc. All rights reserved. February 2010.



2100 Seaport Boulevard
Redwood City, California 94063 U.S.A.
Corporate +1 650 480 8000
Europe +44 2890 416 200
Asia +81 3 5909 6100
<http://www.openwave.com>