



OPTENET WEBSECURE CCOTTA™ APPLIANCE

PROTECTING THE ENTERPRISE IN A WEB 2.0 WORLD



- ANTIMALWARE FILTERING
- MAXIMUM NETWORK OPTIMIZATION
- CENTRALIZED MANAGEMENT
- MASSIVE SCALABILITY

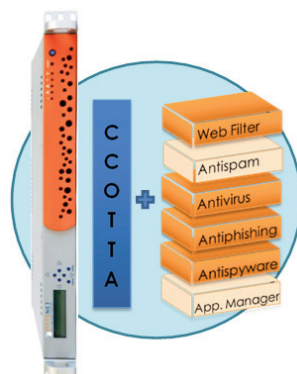
Optenet WebSecure CCOTTA™ Appliance is the fastest and most effective antimalware filtering solution available. Based on a complementary combination of Optenet's WebFilter technology and Kaspersky Lab's engine, it protects corporate IT environments, identifying, classifying and blocking access to web pages that contain unsuitable content or have been infected with malware.

DYNAMIC PROTECTION

The ease with which pages can be created and posted on the Web and the dynamic nature of the Internet mean that content changes rapidly. Most available antimalware filtering solutions base their technology on static URL databases that are left obsolete and ineffective when it comes to filtering dynamic content. The result is numerous blocking errors, preventing access to inoffensive pages or allowing inappropriate content through.

Optenet WebSecure CCOTTA™ Appliance resolves this problem with an extremely powerful solution. A combination of state-of-the-art Optenet technology and Kaspersky Lab's malware engine, helps customers protect their networks, *classify ever-changing Web content with total accuracy*, and ensure a quality Internet experience.

OPTENET'S TECHNOLOGY ADVANTAGE



Carrier Class Optenet Transparent Traffic Analyzer (CCOTTA™) is the heart of Optenet Appliance. CCOTTA™ provides real-time processing and coordination of all traffic through the network to be redirected to the filtering services (such as antivirus and Web filtering) or processed by CCOTTA™ itself. It optimizes the management of all traffic from the Ethernet level and above (L2 through L7).

Optenet's products are developed to work together and share state-of-the-art technology to provide customers the highest rate of **accuracy and dynamic protection for the new Web 2.0** world. Powerful tools include its built-in **Multicontent Inspection & Dynamic Analysis System (MIDAS)** and **Global Intelligence Acquisition Network for Threats (GIANT)** which provides real-time management of known inappropriate content.



BENEFITS

- **Complete protection from online threats** – ranging from inappropriate Web content to viruses, spyware and other malicious code:
 - Ability to set policy based on granular criteria, such as blocking specific sites and file types at certain times of the day.
 - Reduction of IT workload as a result of **central management**.
- **Massive scalability** that allows Web content security to effortlessly keep pace with the organization's business and performance demands.
- Flexible solution that can be combined with other Optenet technology to create custom security solutions, delivered on an **optimized Secure Web Gateway appliance**.
- Ultra high performance that creates a smooth, seamless user experience.
- Automatic updates of new product versions and features.

FEATURES

- **Centralized policy-based management console**, independent of the organization's network topology
- Kaspersky Lab anti-virus engine for protection from viruses, spyware and malware.
- Completely integrated and scalable hardware and software solution.
- Best suited protection for Web 2.0 threats through Optenet's Multicontent Inspection and Dynamic Analysis System (MIDAS).
- Optenet's exclusive **24x7 online content reclassification service**, which ensures minimal overblocking/false positive rates.
- **Powerful reporting tools** for analyzing and monitoring Internet use in real time across the organization.
- Option to **block/manage communications protocols** and applications such as instant messaging, P2P file sharing, chat and VoIP.
- **Easy to integrate with existing infrastructures** (proxies, LDAP, Radius, etc.) in ICAP, RPC or UFP mode, or as a plug-in.
- **Multiple deployment modes:** proxy, bridge, ICAP and router.
- Automatic and continuous updates.
- Alarms and error alerts sent by e-mail and SNMP traps.

CENTRALIZED MANAGEMENT AND REAL-TIME REPORTING

From a single simple-yet-powerful management console, Optenet enables quick and easy policy management for multiple applications across multiple locations and multiple machines. Administrators can use the console to execute and define unlimited security policies that are:

- **Deployable on a global scale**, independent of the network infrastructure.
- **Highly customizable** and can be set up based on many different criteria such as users, user groups, IPs, IP ranges and VLANs.
- Enforceable across **distributed networks** regardless of the geographic location of the end points.
- Easily integrated with profiles defined in LDAP corporate directories, facilitating easier, faster Deployment.

All of Optenet's enterprise solutions include the fastest **real-time monitoring and reporting** system available.

- The reports – supported by a database incorporated into the solution without the need for additional licenses – can be customized for the Enterprise needs.
- Customizable in real-time based on what analysis is required.
- Flexible enough to provide enterprise-wide reporting as well as granular reporting which can include user, location, group, or other classifications – all through the single management console.

CENTRAL ADMINISTRATION CONSOLE

In addition to WebSecure, Optenet can combine a comprehensive range of security services – including antispam – into a single, simple management console. As the organization's security needs increase, services can be added and expanded without the purchase of additional hardware that could compromise the initial investment.



OPTENET North American Headquarters
 2875 NE 191st Street - Suite 901
 Aventura, FL 33180
 USA
 Tel.: +1 800 250 9689

OPTENET European Headquarters
 Paseo Mikeletegi 58
 1^a Planta, Edificio B8
 Parque Tecnológico de Miramón
 20009 San Sebastián, Spain
 Tel.: +34 913 579 150

OPTENET Australia Headquarters
 Level 23, Tower 1, 520 Oxford Street
 Bondi Junction, Sydney, NSW 2022
 Australia
 Tel: +61 (0)2 9513 8882

