



OPTENET MAILSECURE CCOTTA™ APPLIANCE

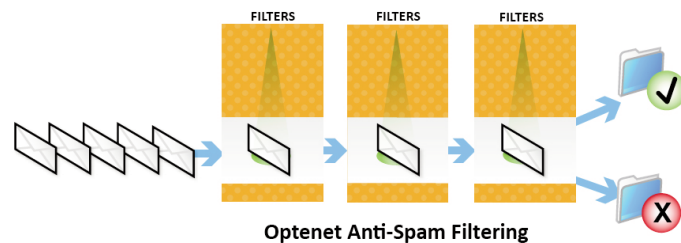
AN INTELLIGENT SOLUTION TO SPAM



MAXIMUM ACCURACY
COMPLETE PROTECTION
CENTRALIZED ADMINISTRATION
MASSIVE SCALABILITY

Optenet MailSecure CCOTTA™ Appliance is the most powerful spam detection and prevention solution on the market. The solution provides highly accurate spam filtering while nearly eliminating overblocking errors. This award-winning combination enables organizations to optimize productivity and network resources without losing critical business information.

Optenet MailSecure CCOTTA™ Appliance is an intelligent, high-performance security solution designed to eliminate and manage email threats for companies that use email as a critical communication tool in their business.



MailSecure features Optenet's start-of-the-art multilayer analysis technology – based on reputation databases, spam detection, Kaspersky anti-virus technology and content filtering – offers and delivers the industry's highest rate of accuracy.

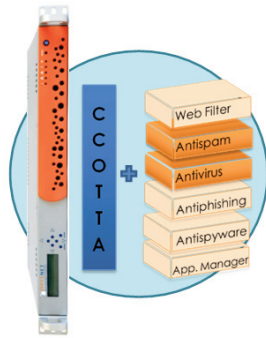
BENEFITS

- Extremely low rate of overblocking or false positives that prevents the loss of critical information
 - Ability to block inappropriate messages before they even enter a company's network.
 - Flexible solution that can be combined with additional Optenet technology to create custom security solutions, and can be delivered either as software or pre-loaded onto an optimized appliance.
 - Ultra high performance that creates a smooth, seamless user experience.
- Massive scalability that allows e-mail security to effortlessly keep pace with the organization's business and performance demands:
- Automatic updates of new product versions and features.
 - Maximum protection against viruses, Trojans and worms, as well as new variants.
 - Incremental, real-time database updates.

FEATURES

- **Reputation-based filtering:** In real time, the system analyzes and manages inbound messages so that inappropriate content is blocked instantly – even before it hits a user's mail server.
 - **Complete content analysis:** For messages that have passed the reputation filter test, MailSecure analyzes the complete context of the e-mail – including origin, URLs within the message, file attachments and more, using **Multicontent Inspection and Dynamic Analysis System (MIDAS)**.
- MailSecure also includes:
- Centralized policy-based management, independent of the organization's network topology.
 - Advanced real-time reporting.
 - Multilingual content analysis in 180 languages.





Optenet Appliance Security Solutions **Carrier Class Optenet Transparent Traffic Analyzer (CCOTTA™)** is the heart of Optenet Appliances. 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).

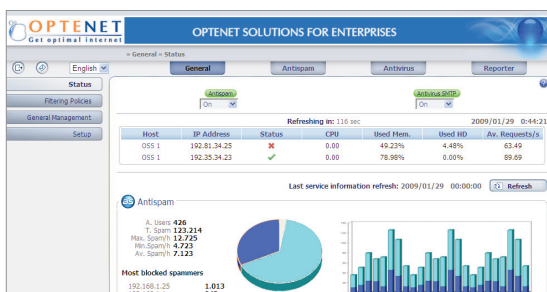
Optenet's products are developed to work together and share state-of-the-art technology to provide customers the highest rate of accuracy and dynamic protection for the new Web 2.0 world. Powerful tools include its built-in **Multicontent Inspection and Dynamic Analysis System (MIDAS)** and **Global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



The Optenet MailSecure CCOTTATM Appliance combines multiple proprietary analysis techniques to deliver a multilayer protection solution capable of detecting spam, viruses and malicious code in email:

1. **Optenet reputation database.** Global list of IP addresses based on the traffic monitored by Optenet on five continents, with reputation value calculated from a number of factors including historic behavior.
2. **Contextual reputation database.** List of IP and e-mail addresses built from what individual organizations believe to be contextually significant, with reputation value derived from historic behavior.
3. **Spammer catalog.** Proprietary system for comparing e-mail addresses with the behavior of individual spammers.
4. **External reputation database.** Global list of IP addresses compiled from traffic monitored by third parties, with reputation value derived from historic behavior.
5. **Falsified address detection.** The Sender Policy Framework (SPF) is a standard designed to prevent falsified sender addresses (spoofing).
6. **Shared lists of suspicious addresses.** Open relation of e-mail addresses with spammer behavior, contrasted individually with third parties.
7. **Gray lists.** Technique based on numerous options available in RFC standards. It blocks e-mails from servers that allow indiscriminate e-mailing.
8. **Verification of URLs in category database.** Tracks and validates links contained within a message.
9. **Multicontent Inspection and Dynamic Analysis System (MIDAS):** Artificial intelligence techniques that classifies and inspects message contents.
10. **URL semantic analysis.** Search and verification through semantic analysis of pages and categories linked to in the body of the message.
11. **Content analysis of URL's.** Search and verification through content analysis of categories linked to in the body of the message.
12. **Proprietary digital signature verification.** This technique extracts the digital signature of a message and compares it with a proprietary database of typical spam signatures.
13. **Shared verification of known spam digital signatures (with signatures for basic mutations).** This technique extracts the digital signature of a message and compares it with the shared database of typical spam signatures.

Through the combination of these techniques, and the information provided by its **Global Intelligence Acquisition Network for Threats (GIANT)**, Optenet delivers the most powerful spam detection service with the lowest rate of overblocking errors and false positives.



The MailSecure CCOTTA™ Appliance offers a single simple-yet-powerful management console that can be customized to meet the needs of any business. Administration features include:

- **Configuration:** set basic configuration values of the service – based on an organization's policies, including maximum email size limits, number of emails per session and more.
- **Trainer:** use real spam emails received within their own organization to train the filtering module to intelligently filter messages, improving the system's effectiveness and accuracy.
- **Challenge message:** lowers the blocking percentage to near zero by sending a reply message to the sender of inbound messages which requires that they identify themselves, thereby verifying that they are a legitimate email sender.
- **Logs:** with log data and statistical analysis, the administrator can quickly and easily verify the state of the solution in real-time, such as the number or type of messages that are being monitored.
- **Updates:** the method for providing updates to the network administrator can be customized according to the needs of each Enterprise.

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
1ª 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

