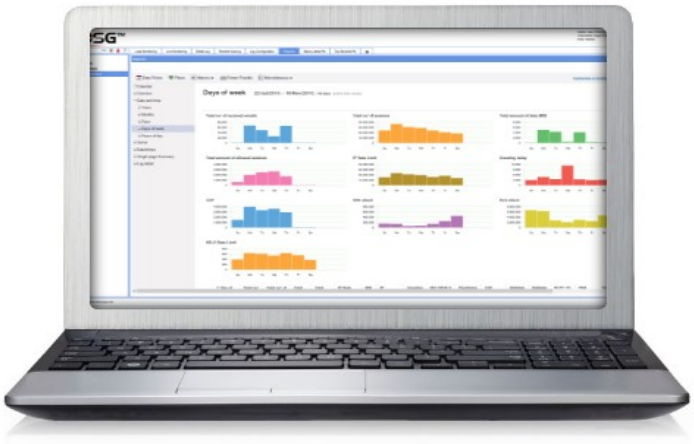
Outbound Spam Guard

CYBONET OUTBOUND SPAM GUARD (OSG) IS A CARRIER-GRADE SOLUTION THAT CAN BE EASILY DEPLOYED TO SCAN AND BLOCK UP TO 99% OF ALL UNWANTED OR MALICIOUS OUTBOUND EMAIL TRAFFIC



OVERVIEW

Easy to deploy, CYBONET OSG functions as a transparent proxy that informs the service provider, in real-time and with granular level statistics, about which IP addresses within their networks are being controlled by botnets. OSG protects an ISP's IP reputation by identifying addresses that are being used spam and preventing those emails from leaving the network. ISPs can proactively identify and remediate IPs and computers that have been compromised by a Botnet. Installed in some of the world's largest ISP networks, a standard 1u server easily handles 2+ Class B subnets and up to 8,000+ SMTP sessions per second, with an ability to process billions of messages daily. Subscriber Transparency - subscribers' services are left unaffected. IP Layer Transparency - no change to the client source IP address. SMTP Envelope and Header Transparency - no trace of OSG processing in email headers.

HIGHLIGHTS

- Transparent solution
- IP Reputation
- Over 12 anti-spam engines
- Recurrent Pattern Detection technology
- IP Rate Limiting
- Optional IP Whitelisting
- Detailed real-time statistics
- Identify spammers within your network
- Prevent IP (and ISP) blacklisting
- Improve service reputation
- Carrier-grade scalable solution
- Neutralize threat of botnets
- Reduce overall bandwidth consumption
- Improve SLAs
- Available as hardware, software and on all virtualized platforms

SOLUTION AT A GLANCE

With global broadband penetration rates increasing and mobile phone/ smartphone technologies becoming more accessible, the burden on ISPs and Telcos to provide reliable, efficient internet services is more complex and more necessary than ever. Service Providers are facing a serious challenge from malicious but organized networks of computers called botnets. Botnets operate within a network, using a Service Provider's infrastructure to distribute massive quantities of spam. Botnets are responsible for the distribution of up to 90% of the world´s spam and strike at a service provider's core business assets; IP addresses and bandwidth.

CYBONET OSG is the ideal solution to neutralize botnet activity within a service provider's network. By harnessing the power of CYBONET's OSG, a service provider can reduce their blacklisted IPs, improve their IP reputation, and reduce the unwanted consumption of their bandwidth.

Real-Time Statistics

CYBONET OSG provides system administrators with real-time and aggregate statistics related to outbound SMTP sessions, including blocking rates of all enabled anti-spam engines, top blocked IPs, alerts of blacklisted IPs within the network, and much more.

IP Rate Limiting

If any attack or email blast occurs from a known, unauthorized IP address, it is automatically blacklisted according to traffic volumes. The system allows you to limit maximum messages and sessions per IP by hour/minute/ second.

Internal IP Reputation System

This highly efficient engine uses proprietary technology to detect and block spam originated from zombies within the ISP's pool at the SMTP session level. Enforcement is applied internally, and the risk of blacklisting, as a result of mass delivery volumes, is reduced significantly.

Recurrent Pattern Detection Technology

RPD technology analyzes large volumes of email traffic in real-time, and is able to detect new spam and malware outbreaks as soon as they emerge, as well as mail sent from botnets (language independent), according to a repeating pattern within the actual mail message.

Transparency

For a service provider, a standard anti-spam or mail relay solution will not suffice. For a solution to be 'carrier-grade', it must effectively filter massive quantities of outbound email traffic without compromising the quality of service that users have come to expect. CYBONET OSG leaves no trace on the original email message and easily fits within the service provider's current network configuration.