

# Sendmail IP Reputation Service™

Real-time Classification of Black, White and Grey Traffic

## OVERVIEW

With unsolicited email comprising over 65% of all email, enterprises and service providers face bloated IT costs and deterioration in the quality of service for valid email traffic. IP reputation helps fight spam and email-borne malware at the perimeter reducing the number of incoming messages at the entry-point before entering the network. IP reputation services are also used to optimize traffic flow so that legitimate message sources gain optimal access, while unauthorized sources attempting to abuse the network are blocked.

## SENDMAIL IP REPUTATION SERVICE

The Sendmail IP Reputation Service is the only dynamic reputation service available to help fight spam and email-borne malware at the network perimeter. Working in tandem with Sendmail traffic control technology and patented Recurrent Pattern Detection™, the Sendmail IP Reputation Service provides an outer layer of protection based on a global analysis of sender behavior. The result is comprehensive protection against attacks, spam, and malware and is proven to dispose of up to 80% of unwanted email at the connection level – saving bandwidth and conserving valuable system resources.

The Sendmail IP Reputation Service leverages the world's most comprehensive email traffic monitoring network to provide real-time analysis of a representative sample of over 95% of the global email traffic and:

- Tracks traffic from over 100 million IP addresses
- Classifies billions of messages per week, in real-time
- Identifies 500,000 new zombies daily

### Analysis of a Zombie

Internet spam activity accounted for by zombies:	85% of global spam, or an estimated 118 billion messages daily
New zombies that come 'alive' each 24 hours:	500,000
Typical number of messages a botnet sends:	Up to 1 billion spam messages in a few hours
Typical number of zombies per single botnet:	10,000-200,000
Number of active zombies per day:	8 million

## BENEFITS

- Dispose of up to 80% of unwanted email at the connection level
- Increases security
- Saves bandwidth
- Reduces system resources
- Eliminates false positives
- Improves detection rates

## BENEFITS

- *Increases security*: Filters the majority of email-borne viruses, worms and trojans before entering the network
- *Saves bandwidth and enhances performance*: Bandwidth requirements are substantially reduced, guaranteeing better Quality of Service for the remaining traffic
- *Reduces system resources*: Reduces second-tier resource requirements
- *Eliminates false positives*: Through rate-limits and temporary rejects, a measured response to threats virtually eliminates false positives
- *Improves detection rates*: Overall (first and second tier) detection rates significantly improved

## HOW IT WORKS

1. The Sentrion™ Email Security Appliance or Sendmail Flow Control™ software queries the IP Reputation Data Center with the IP address of the sender during an SMTP session
2. The Reputation Service replies with risk level classification for each sender
3. The risk level classification is mapped to a defined Sentrion Appliance or Sendmail Flow Control policy, e.g. block or throttle suspicious traffic
4. Graded classes/ risk levels enable intelligent connection management decisions for gray traffic based on:
  - Statistical analysis of averages over time and recent changes of:
    - Mail volume
    - Spam ratio
    - Valid bulk ratio
  - Real-time zombie/botnet detection
  - Continuously refined composite RBL score
  - Use of IP DNS and whois attributes such as:
    - Domain age
    - Geography
    - Known dynamic IP

## REQUIREMENTS

- Sendmail Sentrion Email Security Appliance or Sendmail Flow Control software
- Annual subscription to Sendmail IP Reputation Services

**Sendmail, Inc.**  
 6425 Christie Avenue,  
 Emeryville, CA 94608  
 Tel: +1 888 594 3150  
 Fax: +1 510 594 5429  
[www.sendmail.com](http://www.sendmail.com)