Reflexion Total Control

Product Highlights

Hosted Email Security

- Multi-layered in-depth defense
- Geographic- and language-based filtering
- Address-on-the-Fly™
- In-message control panel
- Identifies address sharing

Outbound Email Auditing

- Outbound antivirus scanning
- Open relay and zombie prevention
- Avoids IP address blacklisting

Volume-Based Protection

- Defeats directory harvesting and denial-of-service attacks
- Supports SMTP restrictions to prevent direct-to-IP attacks

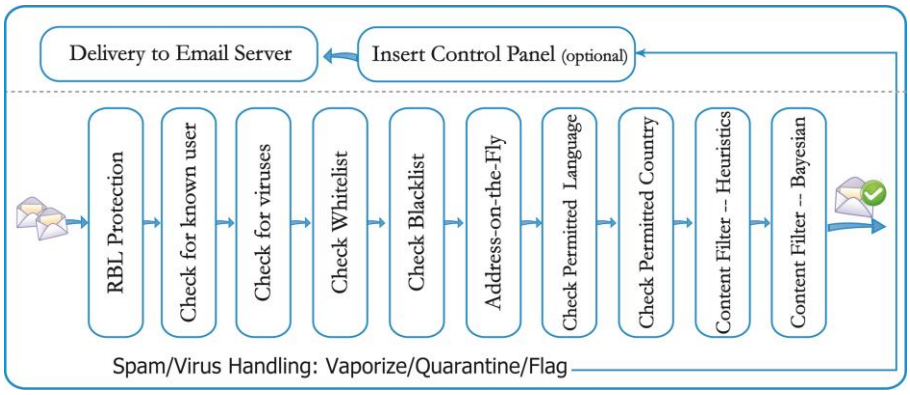
Automatic Email Spooling

- Automatic spooling of all incoming email for 14 days in the event of local power or email server outage
- Optional email archiving, discovery and recovery (see RADAR)

Overview

Reflexion Total Control (RTC) is a hosted email security service that blocks unwanted email before it reaches the corporate network. Reflexion's unique technology also identifies address-sharing and the sources of spam, and provides concrete tools for preserving the integrity of one's primary email address. Automatic inbound email queuing assures email continuity in the event of a local server outage, and outbound email filtering protects one's reputation and helps to avoid the business disruption of IP address blacklisting. Reflexion's service provides the configurability that IT solution providers need to address a wide range of customer requirements, with the automation and simplicity that ISPs require for their subscribers. Implementation simply requires an MX record change.

The following diagram describes the various stages in RTC's defense-in-depth. With its bredth of capabilities, Reflexion's defense is also uniquely configurable, providing the versatility that email administrators and solution providers require to address the widest range of end user requirements. Mail for a specific user will only be subjected to the tests dictated by their configuration. Additionally, the architecture is extensible, so that new defenses can be added as they become available or desirable.



Volume-Based Email Protection

The first two layers of defense are designed to eliminate inbound emails destined for unknown users at your domain – so called directory harvesting attacks. Currently, 80-90% of all messages traveling over the Internet are actually sent to unsers that don't exist at the target domain.

701 W. Randall St., Suite C . Coopersville, MI 49404 . 616.837.6930 . **www.itrw.net**

Permitted Countries

This capability further augments content filtering by blocking messages from any country other than those specifically approved for delivery at the enterprise and individual user levels. Delivery decisions are based on the IP address of the sending server. While some organizations may not be able to use this capability, many domestic businesses may not ever want to receive email that can be determined to have originated outside their home countries or geographic areas of operation.

Total Control Panel

As an option, Reflexion automatically inserts a control panel at the bottom of incoming messages and removes it on forward or reply. This control panel provides a simple and convenient way for users to interact with RTC. For example, users can update their access preferences for a specific sender and address by simply clicking on the intuitive in-message links that are provided. Reflexion's control panel is available in English, Spanish, French, German, Brazilian Portuguese, Dutch, and Italian.

To: user@example.com	Block messages from this sender
From: user@example.com	Remove this sender from my whitelist

You received this message because the sender is on your whitelist.

Address-on-the-Fly™

Reflexion makes it easy for users to employ alternate aliases for a single inbox. Address-on-the-Fly enables users to spontaneously disclose a purpose-specific address on a website, in a discussion forum, in print or conversation, etc., without having to manually configure that address ahead of time. These addresses take the form of a root name plus a suffix of the user's own choosing. For example, to register on eBay, Jane Doe might disclose the address jdoe.ebay@example.com, where the ".ebay" suffix serves as an "email PIN" that assures delivery of email sent to this address. Addresses are independently controllable by policy through simple interaction with the Total Control Panel, so that legitimate users of the address can be "locked down" in the event the address is ever harvested and abused by a spammer.