



# ANTI-SPAM SECURITY MANAGER

Enterprise-class endpoint security  
for Windows devices.

- ✓ SCALABLE SPAM AND VIRUS PROTECTION
- ✓ AUTOMATIC UPDATES SPAM SOFTWARE
- ✓ INBOUND AND OUTBOUND MAIL SCANNING
- ✓ MULTIPLE DEPLOYMENT OPTIONS
- ✓ SIMPLE ADMINISTRATION

**"WE CAN DO IT BETTER,  
FASTER AND CHEAPER THAN  
OUR CLIENTS CAN IN-HOUSE"**

-Steve Jaramillo, Founder and  
Chief Executive, Catalyst

**Security Manager | Anti-Spam filters e-mail efficiently, effectively and affordably.**

Available for servers installed on-site, servers in the NOC, or as a Hosted service the Security Manager | Anti-Spam solution will meet the needs of any business deployment.

With Security Manager | Anti-Spam, administrators block spam by configuring the system and setting global policies centrally then making them available to end-users, who enroll via a web interface.

The Security Manager | Anti-Spam Solution Provides:

- » Customizable and scalable spam and virus protection
- » Automatic updates on spam software
- » Inbound and outbound mail scanning
- » Per-user Bayesian analysis, whitelists, blacklists, rules and quarantines
- » Multiple deployment options
- » Simple Administration

Providing extensive end-user controls, Security Manager | Anti-Spam users can choose from a customizable list of spam filtering options such as high, medium, or low spam scanning, or choose the 'Expert Interface' for more granular controls.

Security Manager | Anti-Spam is a spam protection solution that is being used by companies with 20-120,000 e-mail users.

## KEY BENEFITS

**Multi-tenant** - deployment options exist that enables delegation of administrative duties. The overall administrator is able to create "realms", and realm administrators will be able to create baseline rules, users and streams within their realms.

**Spam detection** - A variety of techniques including keyword search, header analysis, message format analysis, Bayesian statistical analysis, blacklists, whitelists, greylists, open proxy lists, DNS verification, SpamAssassin™-content-filtering rules, sender policy framework (SPF), custom rules and more.

**Hit-and-run detection** - Temp-fails e-mail sent from new senders to cause legitimate servers to retry the message.

**Themeable interface** - Customize Security Manager | Anti-Spam to look like your own web interface.

**Automatic Updates Service** - Ensures you have the most up-to-date spam and virus definitions.

**Configurable Response options** - Tag, quarantine, return or block spam - it's your choice. Can also be set to block certain attachments.

**Fast and scalable architecture** - Efficient architecture minimizes the processing requirement for e-mail content scanning in any size environment.

**Internal and outgoing mail filtering** - can be configured to filter internal and outgoing e-mail.



[www.n-able.com](http://www.n-able.com)

## PROTOCOLS

Security Manager | Anti-Spam works using the SMTP protocol over TCP port 25. In addition it can work in both IPv4 and IPv6 environments simultaneously.

## TEMPORARY STORAGE

Security Manager | Anti-Spam will store messages locally for a period of 5 days by default in the event that the destination server is unavailable. This can be configured to a different length if needed.

## BACKSCATTER

Security Manager | Anti-Spam will issue standard SMTP rejection codes during the SMTP transaction in the following cases.

- » The message has scored high enough to be automatically rejected by Security Manager. The message will be rejected with a 5xx error code.
- » The message has been scanned and hit a rule that indicates the message should be rejected. The message will be rejected with a 5xx error code.
- » The sending system has attempted to send to an unknown user (Users are verified by an SMTP pass through or via LDAP or Active Directory integration and can be configured on a per domain or sub-domain basis). The RCPT TO command will be issued a 5xx error code.
- » The message has already been seen by the Security Manager | Anti-Spam system and the user has manually flagged the message as spam. The message is rejected with a 5xx error code.



## EMAIL SECURITY SOFTWARE

Security Manager | Anti-Spam protects users from seeing other users data, settings and incidents. A regular user will not be able to adjust, manage or otherwise interact with any settings or information on the system that does not relate to their account. Administrators of the system are granted access to manage these settings on the users' behalf.

## PROFILES

Security Manager | Anti-Spam provides the ability for end users to manage their own settings and options. They can manage how mail is detected as spam, if it is to be automatically rejected (discarded), held in a trap or tagged and passed through. Users also can manage their own rules for whitelisting, blacklisting, content filtering, DNSBLs, Bayesian settings and so on. Administrators can set permissions to restrict the settings users have access to.

In specific cases other users can be granted access to manage another user's settings. This is done by explicitly indicating which accounts a user has access to manage. This is done by the administrator of the system.

## AUTHENTICATION AND AUTHORIZATION

Security Manager | Anti-Spam provides built-in capabilities to authenticate end users based on the following methods:

- » Active Directory
- » LDAP
- » IMAP/POP3

This authentication can be configured on a per domain and even per sub-domain basis.

In addition Security Manager | Anti-Spam provides a flexible e-mail security infrastructure to allow for additional authentication and other integration methods to be implemented. These include:

- » Shibboleth (currently implemented at a customer site)
- » SAML2
- » Database Backend
- » Other custom systems

## MAIL STATISTICS

Security Manager | Anti-Spam provides detailed reports about the mail that it has processed. Reports can be generated for the system as a whole or for specific domains. These reports allow Administrators and Site Administrators the ability to see how the system is performing. Reports summarizing the following information are available:

- » Daily mail statistics - How messages were classified on a daily basis.
- » Hourly mail statistics - How messages were classified on an hourly basis.
- » Top Viruses - A list of the most common viruses found.
- » Top Recipients - A listing of the most common recipients of spam.
- » Top Mail Countries - A listing of the countries that send the most amount of spam.
- » And many more.

These reports can be generated on an as-needed basis or can be configured to be automatically generated from within the Security Manager | Anti-Spam anti spam program and emailed as PDF attachments.