White Paper

Focus on What Matters: How to Reclaim your Email Using Whitelists

There is a modern proverb that goes something like this:

Acknowledge the bad, but focus on the good.

In sum: do not be so naive as to think that bad things do not exist in this world, but rather choose to spend your energy and time focusing on the good things instead. Make a conscious decision that focusing on the good will not only get you further in life, but ultimately make you happier.

Before we get too carried away here – no, this is not a self-help, positive thinking piece - in the world of technology, IT professionals spend more than their fair share of time focusing on the bad, and it is often out of necessity. Every security decision comes with its own set of trade-offs, and IT professionals are often choosing the lesser of two evils.

But, the sentiment behind this saying poses an interesting question: can focusing on the good ever make you more secure?

Introduction

The answer, is yes.

And in fact, there are situations where it is both in the best interest of a company's *security* and *time*, to focus on the good.

The criteria below can readily help identify those situations where it is in the best interest of *time* to focus on the good:

1. Does the number of "bad" items/people/situations outnumber the "good"?
2. Is it easier to identify the "good" than it is the "bad"?

Now when the above criteria is met, one must simply ask the question: will my company be any less secure "focusing on the good?" (more on this to come)

One set of circumstances where the above questions can both be answered with a "yes" is email. And if we ask ourselves the question: will focusing only on the good email I want to receive make my company less secure, we are certain that if you read on, you will find the answer is "no."

If your organization was able to receive every message it wished to from a safe email sender, and messages from an unsafe sender were simply ignored, you would be probably be hard pressed to find a security threat in this mix. Some IT people might even describe this as a utopia.

However, the solutions we have in place to protect our email messaging systems typically do not adhere to the principle above. Rather, they hone in on the "bad" (see table 1.1).

The methods range from the mainstream (content filters) to the paranoid (disposable email address services). They all offer some degree of control over abusive email, but none are perfect and many are time consuming.

A New Approach

So here we are - 32 years into the problem of spam,[1] billions of dollars deep into the problem of solving it, but still haven't been able to eliminate it.

In 2009, "spam" email comprised 81% of all messages sent.[2] And while some general characteristics can be used to describe what the messages that comprise this 81% figure may have looked like (illegal html, all capital letters, invalid recipient field etc.), the truth of the matter is that the characteristics of spam are continually evolving.

In addition, every day nearly 150,000 new zombie computers are created[2] and an average of 10,000 new malicious code signatures are added to software vendor Symantec's threat database.[2]

Table 1.1 - Method v. Methodology

Email Protection Method	System Methodology
Content Filter	Criteria is set for what is "**bad**" content - messages filtered accordingly
IP Reputation Service	Criteria is set for what a "**bad**" ip source is, messages filtered accordingly
Blacklist	Criteria is set for what a "**bad**" sender is, senders grouped in a database and messages filtered accordingly
Disposable Email Address Services	Keep your email address out of the hands of the "**bad** guys" at all costs

1 Wikipedia, Mar 10, "Gary Thuerk"

2 Royal Pingdom, Jan 10, "Internet 2009 in Numbers"

Focus on What Matters: How to Reclaim your Email Using Whitelists

In sum: the ways in which the "bad guys" present themselves, and the methods they use to try to present themselves, are continually evolving.

So if the characteristics of 81% of email traffic purposefully vary on a continually basis, is there any constant in this equation?

Yes: the "good" guys.

The sending source, sending address, headers and general content you receive from email senders you communicate with on a regular basis has remained relatively constant. Namely because there is little incentive for your colleague, mother, best friend, boss, personal trainer, roommate, or child to manipulate the properties of email.

They have a message they wish to send to you, and they do exactly that. The systems they use to send these messages to you all act alike and the email addresses they utilize are generally unvarying.

Now if you had to choose, would you prefer to sift through the 90 trillion emails sent in 2009[3] looking for the roughly 81% that were "bad" or the 19% that were "good"?

If we happened to be so unlucky as to be tasked with this mission we would focus on the latter. We would build a simple set of criteria to identify who comprised the 19%. We would acknowledge that the 81% existed (to do otherwise would be reckless), and where it made sense examine these messages more closely. But we would focus our energy and strategy on the *good*.

We would build a *whitelist* (see table 1.2).

Table 1.2 - Method v. Methodology (Part 2)

Email Protection Method	System Methodology
Whitelisting	Criteria is set for what is a "**good**" message, messages filtered accordingly

Whitelists are simple but powerful tools organizations can use to manage their email. When leveraged properly they deliver an unprecedented level of security for an organization while ensuring a more productive email experience for the end-user.

Here, we will briefly explore **what a whitelist is**, the **need for sender *source* whitelists** and **sender *address* whitelists**, the **characteristics of a good whitelist**, the **role of the user in managing a whitelist**, and finally the **role of the IT administrator in the whitelist management process.**

What is a whitelist ?

A whitelist is a list of entities you trust and, as a result, are given preferential treatment. Our discussion here will be limited to sender *address* and sender *source* whitelists. A **sender address whitelist** "is a list of contacts that [a] user deems are acceptable to receive email from and should not be sent to the trash folder".[4]

Likewise, a **sender source whitelist** is a list of *sources* a user deems acceptable to receive email from.

You've probably been using whitelists in one form or another for years now: LinkedIn, Facebook and every major IM client operate using whitelists. In each of these cases connections/friends/buddies that are on your "whitelist" (friend list) are given preferential treatment when interacting with you - and generally confirmation of some sort is required to join an individual's whitelist

What it isn't: a commercial list. Commercial whitelists are used by some internet service providers (ISPs) to allow a subset of senders (usually commercial) to bypass spam filters when sending email messages. There is a fee involved to get on the whitelist, either annual or per-message.

These whitelists are not based on who isp users are actually interacting with and as a result are inherently ineffective as a whitelist (but more on this later, see the *characteristics of a good whitelist*).

Sender Source & Sender Address Whitelists

While both sender *source* and sender *address* whitelists offer varying levels of security individually, when combined they afford the IT department and end-user the greatest degree of security and control over the inbound message stream.

Examining the source of an email message is a great opportunity to take a first pass at determining whether a message is "good." And there are a number of simple tests an email protection solution can perform to determine whether the source of a message is operating as "good" sources should (certain forms of greylisting are one such example).

A whitelist compromised of sender *sources* is also an opportunity for an IT administrator to decide on a broad level whether messages from certain ip addresses should always be accepted. While these types of entries on a whitelist may be rare, the control they offer is highly beneficial when needed.

Assembling a whitelist of sender *sources* will make the tasks of assembling a whitelist of sender *addresses* that much simpler: the pool of messages a whitelisting system must sift through to assemble their safe sender list will be smaller and will already bear the first mark of approval as "good."

A sender *address* whitelist provides a critical level of granularity in the process (down to a single domain or email address). There are two critical types of sender *address* whitelists: **company-wide lists** and **personal-users' lists**. Company-wide address lists will include all those email address an IT administrator deems safe on a **company-wide basis**. Contacts that are placed on the company-wide sender list will always be accepted.

A personal-user's address list allows for further refinement on a **per-user level** during the whitelisting process. And when needed, allows end-users to make individual decisions as to who they would like to communicate with.

A robust and dynamic set of sender *address* whitelists puts the company and its users in control: they know exactly who they want to communicate with and, as a result, can silence the noise of "spam."

3 Royal Pingdom, Jan 10, "Internet 2009 in Numbers"

4 Wikipedia, Apr 10, "Whitelist"

Focus on What Matters: How to Reclaim your Email Using Whitelists

Characteristics of a Good Whitelist

So, "great" you say – this all sounds well and good, but to compile the lists just described would take months. Yes, to **manually** build these lists would more than likely be a waste of time and resources.

For a whitelisting system to work, it must have a way to populate itself automatically, among other things. A good whitelist must be:

1. **Automatically Assembled**
2. **Dynamic in Nature**
3. **Easy for "Good Guys" to Join**
4. **Hard for "Bad Guys" to Join**

We'll explore each of these briefly.

Automatically Assembled

A good whitelist must have a way to populate itself automatically. This means the system must have a way to automatically evaluate both the ***source*** of a message and the ***sender*** of a message to determine whether they are "good."

Evaluation methods must be definitive in nature and avoid at all costs excluding "good" senders from joining the whitelist.

Good examples of simple – but highly accurate – sender ***source*** tests include:

- **Sender System Tests** – Does the sending server operate as a normal server should, sending **and** receiving messages? Basic smtp retry tests can assess whether the source of a message originates from a "spamming" server, or a legitimate mail server.
- **Familiarity Tests** – has the sender associated with the message source ever sent a message prior? If so, is the sender already whitelisted?

Good examples of simple – but highly accurate – sender ***address*** tests include:

- **Outbound Messaging Tests** – has the email user ever sent an email to the sender before? A good whitelisting system will automatically whitelist all outbound message recipients as a best practice.
- **Current Contact Tests** - is the sender already in the system? A good whitelisting system will allow for contact import prior to deployment.
- **Confirmation Requests** – will the sender respond to a confirmation email? Spammers will not, legitimate senders typically will.

These tests should always be supplemented with the end-users' direct involvement. While the bulk of entries on a whitelist will be automatically created by the system, users and administrators should have the ability to intervene and manually create & remove whitelist entries in certain circumstances (e.g. when a user no longer wishes to block a particular person or an administrator wishes to whitelist a domain or ip source).

Dynamic in Nature

A good whitelist is never complete. A good whitelisting service must have mechanisms in place to perform source and sender tests instantaneously and continuously.

Whitelists that are dynamic in nature will ensure false positives ("good" messages that are classified as "bad") are kept at a minimum and will provide for the most productive email messaging experience for users.

Easy for the "Good Guys" to Join

A good whitelist must have a way for legitimate email senders to join it. Ideally the method you select to allow new senders to whitelist themselves should be neither time consuming nor cumbersome.

If you choose to use a confirmation request to allow new senders to join, the email message requesting confirmation should be clearly written and succinct. The action required by new senders to join the whitelist should be simple to perform (e.g. reply to the message).

In the case of Facebook or LinkedIn, "friend request" confirmations are sent out via email and users are asked to confirm connections via web links.

Hard for the "Bad Guys" to Join

While you'd like to make life as easy as possible for those legitimate email senders wishing to reach your business, ideally you'd like to make it impossible for the "bad guys" to join.

When selecting a method for new senders to join your email whitelist you will want to ensure it is as difficult as possible for the "bad guys" to complete the authentication process.

A confirmation requirement to join the whitelist (that requires recipients to respond to the message in order to join), is a good example of an authentication process that will be nearly impossible for the "bad guys" to complete.

Spammers will be unable to complete the process for a number of reasons:

1. **It would require that they give up their anonymity.** Spammers are breaking the law – remaining anonymous is the only way they can stay in business.
2. **It would require time on their end.** Spammers are not interested in any single message getting through - they are focused on the larger message stream.
3. **It would require resources.** Many spamming servers are not even configured to accept mail in return (an expensive resource drain) and confirmation messages typically won't have to be sent.

In sum: whitelists do work, but they can only excel when the above criteria are met. A whitelist is only as good as its implementation.

Focus on What Matters: How to Reclaim your Email Using Whitelists

A User's Role in Whitelist Management

IT departments are tasked with protecting their users, protecting the company, and at times, protecting the company from its users. This latter task can at times leave end-users on a tight leash at the expense of company security and end-user productivity.

However, in the case of whitelist management, **users must play a role**.

A successful email whitelisting tool should allow users access to the following:

- **A view of their own personal message stream in its entirety (sans any infected messages)**
- **The ability to easily add and remove individual contacts from their personal whitelist**

The end-user will ultimately be the only one that can determine whose messages are "wanted" and whose are "unwanted." By allowing users the above functionality an IT department can increase the effectiveness of a whitelisting service significantly.

Rather than sequestering email users away from the process of managing email, introduce them to it. Make them your ally, not your enemy.

An IT Administrator's Role in Whitelist Management

At this point, some may be wondering where the IT administer fits into the whitelist equation, and how much time is really required on the part of an IT administrator or IT department, to make email whitelisting work.

The answer is of course "some" – but not a lot.

Active (adj): marked by or involving direct participation

Passive (adj): receiving or enduring without resistance

Security solutions typically adopt either an active or passive approach to protecting any given system or network entry-point.

In terms of email security, an active approach aims to prevent attacks from compromising an email system in the first place, whereas a passive approach addresses threats once they've already been recognized.

There is room for both active and passive components within any comprehensive security strategy.

Anti-virus scans, anti-spoofing checks, and ip reputation tests are all examples of passive services (mechanisms that seek to stop threats once they are detected).

Whitelisting seeks to eliminate the opportunity for "bad guys" to have any degree of access to the network and can be classified as an active approach to email system protection.

As an active apparatus whitelisting typically involves a greater time investment at the frontend of the deployment process, but typically requires very little on an ongoing basis (in comparison to passive protection mechanisms).

(Cont)...

This means an IT administrator's role is greatest during the very first stages of launching an active solution, but once it is up and running an administrator need only play a limited role.

During deployment an IT administrator's role will be to manage the following:

- **Contact import:** populating the system with any pre-existing company contacts
- **Configuration**: setting up any company-wide whitelist contacts, domains or ip ranges your organization wishes to accept across the board

Investing this small amount of time on the frontend will ensure exponentially better security on the backend, and provide significant time savings over the life of the solution.

Acknowledging the Bad

Before we conclude, let's briefly take a moment to "acknowledge the bad" - now that we've spent some time discussing how to focus on the good. Taking a moment to do so will make the task of "focusing on the good" that much more productive for IT staff and end-users alike.

While whitelisting allows an organization to focus their resources heavily on those they would actually like to communicate with (rather than those wish not to), to simply ignore the "bad guys" entirely dodges a great opportunity to ease the task of "focusing on the good." The following best practices allow an IT department to briefly "acknowledge the bad" and will afford a greater level of security across the entire organization:

- **Inbound and Outbound Anti-virus Scanning**: ensures messages entering your network are not infected with a known virus (because even the "good guys" may accidently send a dangerous message)
- **Recipient Checking**: ensures messages entering your network are addressed to a valid recipient in your email directory (because what's the point in even accepting those 1234@yourdomain.com messages?)
- **Anti-spoofing check (SPF & DKIM)**: ensures spoofed messages that claim origin from a domain that is forged, are stopped (because why would you want messages from a forged sender?)
- **Encryption**: ensures both inbound and outbound email communications are secure from "eavesdropping" (because you don't want the "bad guys" listening in on your conversations)

The majority of these checks should occur just before a whitelist check kicks in. Think of it like a first round of interviews for a new job: the individual that shows up in flip-flops and whose resume is lacking critical experience for the position being filled may be weeded out immediately. It is then easier to focus on the remaining "good" candidates (or "good" email messages in this case) to pick just the right ones to accept for a position (or deliver to an email inbox).

Focus on What Matters: How to Reclaim your Email Using Whitelists

Concluding Thoughts

When implemented correctly, email whitelists are the most powerful tool available today to secure your email system.

Whitelisting email protection systems avoid the pitfalls of many of the other email protection methods available and, by doing so, offer an unparalleled set of benefits:

- **Total control over email**
- **No lost email messages**
- **A vastly more secure email environment**
- **A highly productive messaging experience for users**

Email continues to be the most widely used business communications tool today and, as a result, the attacks on it are continually mounting. Rather than continue to engage in an endless battle against the "bad guys," it's time to simply focus on the good ones.

We hope after you finish reading this you take a closer look at the email protection mechanisms you have in place: are there whitelisting features you are not already using that you could activate? Do they adhere to the qualities of a good whitelist outlined above? How much time do you spend dealing with email-related problems every day? How much time do your users spend managing unwanted email?

If you aren't satisfied with your answers to the above, it may be time to migrate to a more robust whitelisting solution. Take the plunge, and **focus on what matters**.

About Sendio

Sendio is a feisty Southern California software development company whose products protect the email environments of enterprises and institutions from attacks and abuse. Using self-managing communities similar to those found in modern social networking applications, Sendio users receive all of the email sent by customers, suppliers, partners, associates and other members of their "community" while being completely shielded from both nonsense messages sent by casual abusers and devious messages from malicious criminal concerns. More information regarding Sendio can be found at sendio.com.

877.363.2772 • www.sendio.com