Why Use an SMTP Relay Service?

The Benefits of Scanning Outgoing Email
Before It Gets Delivered

MAILCHANNELS

Why Outsource Email Delivery?

You've got a web hosting company to run. Whether you're one person with two shared servers, or a global powerhouse with dedicated outbound email gateways, it's a constant challenge to make outbound email work reliably for your customers. Dealing with spammers and the problems they cause eats up valuable IT and support resources, which you could be investing in growth and customer satisfaction.

What do you do if cyber criminals suddenly exploit 200 WordPress accounts and start sending two million spams per hour across a swathe of your IP space? What if Spamhaus lists your entire network or puts your company on the ROKSO list? What if AOL blocks you and you can't get through to their support line to x the problem? What if you can't get them to take your email, no matter what you do?

A hosted SMTP relay service solves all these issues and more.

Email is the most widely used application on the Internet. And the use of email in the web hosting environment just continues to climb. Whether it's WordPress sending out password resets, or individuals using their webmail accounts, customers absolutely expect that email will get to its destination with reliability.

An SMTP relay service guarantees that sent emails arrive in their recipients' inboxes.

This white paper explains the challenges of sending outbound email and maintaining the infrastructure to do so. It also explains the benefits of having a trusted partner manage this process for you, and why those benefits extend beyond reliable email delivery to include enhanced security, trust and reputation.
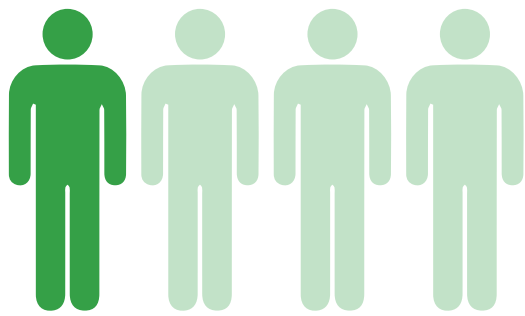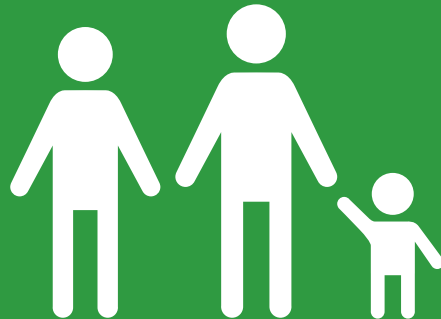
25%

Of support tickets are caused by email delivery issues.

Source: MailChannels customer survey, June 2015

What would your team do with an extra 10 hours per week?

Spam is the Only Constant on the Internet

Email receivers are on constant lookout for sources of spam. IP blacklists give them an easy and effective tool to block unwanted content from sites that don't keep their own users secure from hacking. Even if you feel your operational security is strong, your vigilance may not prevent your network from being hijacked to send spam. Just a single compromised user account can get a server blacklisted by a major email receiver — or even the entire Internet. Your email traffic is at risk because spam is a persistent threat.

Just a single compromised user account can get a server blacklisted by a major email receiver – or even the entire Internet.

If Spamhaus blacklisted your entire network (or a large part of it), the result would be a complete halt in email delivery for all your customers. Think about the social media backlash that could follow such an event and how it would impact your company's reputation.

Do you have a strategy for what happens if your servers are blacklisted? What would email delivery problems cost you in terms of support and customer satisfaction?

With a hosted SMTP relay service, the constant problem of outbound spam is handled for you. The monthly fee is minor compared to the advantage of offloading the management of IPs and RBL listings to a partner that specializes in email deliverability.

How SMTP Relay Services Work

An SMTP relay service analyzes all the email leaving your servers, detects the spam, and blocks it. Legitimate mail is delivered through thousands of carefully managed IP addresses that you don't have to worry about because they're run by anti-spam experts. Best practices for outgoing email security are enforced to ensure compliance with the strictest requirements of email receivers and blacklist operators.

The solution also processes real-time feedback and error messages from email receivers to pinpoint the accounts within your network that are spamming. Spam traps are located and avoided. And it all happens automatically.

Parsing receiver feedback is part of the solution. Receivers provide valuable clues as to what they think about the email you are sending, so it's critical to listen to what they have to say. This is how we break it down at MailChannels:

1. The first step is using real time response analytics to assess reputation, content or behavioural problems. It's difficult to monitor blacklists in real time (believe us, we've tried). Often the most timely feedback is from the receivers while you try to deliver email. Some receivers maintain private blacklists based on feedback from their users; you can't monitor this type of blacklist.

2. Another type of feedback comes from spam traps. These are email addresses that have fallen into disuse and are now being used to build automated blacklists. They are triggered simply by trying to deliver a message to that email address.

3. Receiver feedback is also provided in the form of FBL (Feedback Loop) reports. FBL reports are structured email messages sent by administrators at a receiver's network usually in response to complaints from recipients.

We've classified responses from millions of receivers and trillions of messages so that we can determine with a high degree of accuracy whether a specific delivery attempt is encountering IP reputation issues, triggering a content filter, or hitting a spam trap.

Plus, we promote feedback directly from email recipients by sending messages with links to provide a channel for receiving complaints about abuse. Some email clients will actually render these links in the user interface to allow recipients to "Unsubscribe" or "Report Abuse".

We track all this information in real time and use it to optimize delivery, assign reputation and alert customers about abuse in their networks.

The MailChannels Difference

At MailChannels, we know how to apply best practices for excellent email deliverability, automatically. Our experts are world leaders in machine learning technology and approaches to identify spammers based on their behavior, which is how we stop spam email from sullying the reputation of our IP addresses.

98% of IP addresses managed by MailChannels are ranked as Good or Neutral by Cisco SenderBase.

We also provide tools to help our customers improve their own security. We'll notify you when a user, script, or server is infected by spammers and provide a webhook API to let you shut down the spammer on your end automatically. Spam isn't the only reason cybercriminals might exploit your servers and users, but knowing when they do is an easy and quick way to improve your security.

Tools That Give You Real Network Insight

Tracking down and resolving email delivery issues can be a frustrating and time consuming process for hosting customers and support staff.

Typical mail server software forces you to search through text-based log files and to interpret obscure response codes from receivers. It's difficult or impossible to break out statistics about your outbound mail in order to discover who's sending the most, and which users might be getting in trouble.

MailChannels addresses all of these problems and more, with visibility tools that extend form your support desk all the way out to your end users:

- **Lightning-fast search** that lets you located any email delivery attempted out of your network. We index every conceivable data point around every message delivery, enabling you to search by subject line keywords, recipient address components, and across date ranges – just to name a few of the parameters available.

- **Real-time reporting** lets you see which IP addresses, users and apps have generated the most email volume, spam, and rejected email from your network. The top senders report feature lets you quickly assess which customers are generating the most volume, or the most problematic email traffic.

Hint at developing trends where network operators and hosting providers can get certified for implementing compliant outbound infrastructure.

Take the Mystery out of Deliverability

When you outsource your email delivery to MailChannels, we worry about IP addresses and RBL listings for you. It becomes our problem because that's our job.

Here's how we do it:

1. **MailChannels uses huge infrastructure** that delivers email for hundreds of customers with extremely high reliability. We run replicated services in at least three geographically separate data centers and use load balancing at every tier to ensure continuous uptime. Our uptime and SMTP connection latency is totally transparent and visible to you at any time by visiting status.mailchannels.net.

2. **We provide 24x7 email support** with an average response time of 20 minutes to all classes of tickets. Get answers to email delivery questions at any time of the day or night within minutes. If you need even more assurance, you can purchase premium support with strong uptime and support response guarantees.

3. **Outbound email is our business. It's all we do.** MailChannels is the world leader in providing multi-tenant outbound email service, and our entire R&D effort is focused on getting better at this every day. No other provider can match our capabilities for spammer detection and reliable email delivery for multi-tenant email.

The greatest benefit to you is the peace of mind you'll have, knowing your IP reputation is protected and your customers are satisfied with your level of service. MailChannels Cloud will enhance trust in your reliabiliy as a hsoting provider or network operator. When spam is the only constant on the Internet, having an outbound infrastructure that's certifiably compliant with global anti-spam standards is a business asset.

site5

"I've been happy with MailChannels since we started using it and I know our Abuse Manager is as well. It has freed up a ton of time for their team. Plus, we've seen a huge reduction in support complaints regarding mail delivery issues."

GRAHAM McMILLAN, CTO, Site5

Let us manage IPs and RBL listings for you

It takes about five minutes to sign up for MailChannels Cloud, configure your servers, and stop spam from leaking out of your network.

Pricing is based on outbound email volume; packages start at $49.99 per month for up to 40,000 messages. Contact us for an estimate.

About MailChannels

MailChannels provides outbound email filtering and email delivery solutions for service providers. The company improves the reliability of email delivery for shared hosting, dedicated hosting, VPS hosting, cloud hosting, and Internet service providers that struggle with IP blacklisting and spam issues. MailChannels Cloud is an email relay service that relieves businesses of the cost and complexity of managing IP blacklisting and outbound spam.

MailChannels is an active member of the Messaging, Malware, and Mobile Anti-abuse Working Group (M3AAWG), and the Anti-Phishing Working Group (APWG).

Next Steps

Sign Up for MailChannels Cloud

Related White Papers

Lawfully Filtering Outbound Spam in the European Union
See All Resources

Explore Other Resources

Request a Live Demo
Help Center
Customer Success Stories