



Abusix Mail

Email abuse management built on empirical threat intelligence.

Every day, 3.4 billion phishing emails go looking for a way in, and close to half of all email traffic is now spam. Most blocklists answer that by policy: infrastructure gets listed because it falls into a category someone decided should be blocked, whether or not anything inside it has ever sent an attack.

That is where your false positives come from, and they do not stay in the backend. They reach your customers as blocked invoices, failed logins and support tickets your team has to explain.

Abusix Mail works the other way round. A global proprietary sensor and spam trap network watches live attack traffic 24/7, processing over 250 million signals a day. When an IP, domain or URL is seen sending spam, malware or phishing, it is classified on that observed behavior and published to our DNSBL within a tenth of a second. A built-in Welcome list keeps known-good infrastructure from being listed by mistake. Every entry traces back to a real, observed attack event.

Better reputation, higher inbox placement

- ✓ Reject at connection time, before filtering and storage
- ✓ No hardware scaling to inspect mail you never wanted
- ✓ Threat reputation updates within 1/10th of a second
- ✓ Delisting processed in under two minutes
- ✓ Self-serve delisting, handled by our team, not yours
- ✓ Runs on the mail stack you already have

99.6 %

Catch rate across the full blocklist surface.

<0.284%

False-positive rate

55 %

Reduction in spam complaints

+94 %

Inbox placement

25 %

Lower cost than comparable blocklists

Observed Malicious Behavior: Empirical Threat Intelligence at Mail Scale

We built Abusix Mail on a single principle: every listing must be earned through direct observation of malicious behavior. A global sensor and spam trap network captures live attack traffic 24/7 across the internet, processing over 250 million signals a day. When an IP, domain or URL is observed sending spam, malware or phishing, it is classified on that behavior and published to our DNSBL within a tenth of a second. New botnets are detected within minutes of first observed activity.

That is the opposite of how most blocklists are built.

Curated, policy-based blocklists add infrastructure because it falls into a category, and they lag behind the attack infrastructure actually in use today. You inherit their editorial judgment, including the parts that block your customers' mail.

With Abusix Mail, a built-in Welcome list sits underneath all of it, keeping known-good infrastructure from being listed by mistake. It is a structural solution to false positives, which is why our customers see false positives drop by over 40%.

Our coverage spans the full mail threat surface: IPs, domains, email addresses, URL shortener links, links to cloud storage content, cryptocurrency wallets, and attachment hashes. Competitors who sell domain blocklists cover a fraction of that, and you typically experience this gap when it surfaces as a customer complaint report.

The Abusix Global Sensor Network feeds more than 10 blocklist datasets, and the verdict happens at the first decision point: your MX queries the DNSBL, threats are rejected at the edge, clean mail is delivered. Your architecture stays as it is, while the same intelligence screens outbound traffic.

The result is a 99.6% catch rate at a false-positive rate under 0.284%, with over 99% of spam blocked and 9.5 billion threats stopped a day. More threats get blocked at the edge, and less legitimate mail gets impacted.

Block what actually attacks, and nothing else

- ✓ Reject known-bad senders at the SMTP edge, before filtering
- ✓ Cover IPs, domains, email addresses, links, attachments, etc. with 10+ blocklist datasets
- ✓ Screen outbound mail too, so your own network never quietly burns your reputation
- ✓ Delist in under two minutes, with self-serve support we run for you
- ✓ Pay on average 25% less than comparable blocklists

Abusix Mail Key Features

100% Empirical Listings

Every entry is earned through observed behavior, not an editorial category rule. If an IP, domain or URL is on the list, we watched it send an attack, and the listing traces back to that event.

Built-in Welcome List

Known-good infrastructure is protected from being listed by mistake. This is the structural reason our false-positive rate stays under 0.284% while the catch rate remains at 99.6%.

The Widest Threat Surface in the Category

More than 10 blocklist datasets covering IPs, domains, email addresses, URL shortener links, links to cloud-storage content, cryptocurrency wallets and attachment hashes. Competitors selling domain blocklists cover a fraction of it.

Real-Time Reputation

Threat reputation updates within a tenth of a second of a signal hitting the global trap network, and new botnets are detected within minutes of first observed activity.

Protects Both Directions

Filter what arrives, and optionally screen what your network sends out. Catching a compromised account on the way out is what keeps your IP ranges off everyone else's blocklist.

Delisting in Minutes

DNS zone files rebuild every minute and delisting is processed in under two minutes, so a mistake costs you minutes instead of a week of goodwill.

Self-Serve Delisting Service

Hand us the delisting queue. We handle the requests, the verification, and the human support, with security measures that prevent the process from being exploited.

Nothing to Deploy

No appliance to rack, no agent on endpoints, no proxy in front of your mail. Works with Postfix, Exim, Sendmail, Qmail, Rspamd, SpamAssassin, Microsoft Exchange, Zimbra, cPanel and Plesk, plus Barracuda, Cisco and Symantec gateways, and any SMTP server that supports DNSBL lookups. Each has its own setup guide, and none needs a services engagement.

Test Abusix Mail

Test how empirical threat intelligence works by activating your free trial.

It only takes a few minutes to get started. You only need to point your edge mail servers at our DNSBL for you to measure your coverage gap on your own traffic.

[Start free trial](#)

Trusted by 7 of the 10 largest European telecommunication companies.

About Abusix

Abusix is the leading network security company that offers solutions for email security and network abuse report handling, blocks email threats with empirically earned threat intelligence, and automates network abuse handling from first report to resolution. Seven of the ten largest European telecommunications companies are Abusix customers. Learn more at abusix.com.