

Abusix Mail Intelligence

Keep Malicious Messages Out of Your Mail Server
and Your User's Inboxes

OVERVIEW

Mail system operators see as much as 95% of the mail hitting their mail servers as spam and fraud, thus need the first line of defense for their server and user's Inboxes. Abusix is recognized as the most effective commercial blacklist for blocking spam, fraud, and suspicious senders, in the market today.

Over 20 Billion Threat Indicators Processed Per Day

DESCRIPTION

Abusix provides Mail Intelligence to mail operators, security providers, and enterprises to allow them to block mail-borne threats and protect their customers. Using our proprietary sensor networks, Abusix has an unparalleled view of threats. Our detection and blocking of compromised IP addresses and domains found recurring in spam at the edge, allows upstream message heuristics and antivirus engines to run more efficiently.

A FEW OF OUR CUSTOMERS



KEY BENEFITS



1. Abusix Mail Intelligence (AMI) blocks real-time emerging threat identification in less than 10 seconds, where our competitors' block new emerging threats by 10 minutes or more.



2. AMI provides simple fast drop-in integration into your existing mail servers and antispam filters.



3. AMI costs on average, 25% less than similar competitors, and provides rapid ROI through both direct cost savings and through a dramatic reduction in malicious traffic.



Spam Catch Rate: 99.02%
Malware Catch Rate: 99%

MAIL INTELLIGENCE DATA IS POWER

Block sophisticated mail-borne cyber-attacks:

Mail Operators

- Our broad sensor network allows us to detect compromised IP addresses and domains sending spam faster
- Our state of the art architecture process and identifies new threats in 1/10th of a second validates and issues a final decision in less than 10 seconds across DNS.
- Better source data provides a 3x increase in blocking of known malware at the edge than other blocklists.

Network Service Providers

- Transparent blacklisting, delisting process, and support resolution helps relieve your postmaster of work
- One stop information source allows network administrators to understand the reason for a block, thus giving them a clear signal to help a user on their network or shut down an open relay, bot or bad actor.
- Clear delisting processes help legitimate senders understand their problems and thus secure their outbound servers faster.

Security Vendors

- AMI relieves the security vendor's anti-spam and anti-virus filters of the noise and the need to evaluate mail from known sources of spam; thus freeing up these filters to work on the harder more specific problem.
- AMI is designed to help the legitimate sender who has a bad configuration understand what they need to do, to make email work better.
- AMI is also, specifically designed with the security vendor reseller model, in mind.



"Because of its high SPAM catch rates and low False Positive rates, switching to Abusix Mail Intelligence was a no-brainer. Working with a bunch of fun, smart people, doing really cool stuff and who have great ideas is just icing on the cake."

- Abusix Mail Intelligence Customer

ABOUT US

Based in the United States with operations in Germany, Canada, Argentina, and Brazil. Abusix has long been considered one of the world's leading authorities on tracking and solving network threats. Abusix Raw Intelligence provides an unparalleled view of threats. The Abusix Mail Intelligence service, our blacklist processes and curates our Threat Intelligence and other threat research, facilitating real-time lookup of IP, Domain and URL reputation for various applications and services. Abusix's SaaS service, AbuseHQ centralizes and correlates all security and abuse reports, alerts and events from sources that originate from 3rd parties and from network provider hosted subscriber network ranges.



Contact us to learn more about
Abusix Mail Intelligence Feeds.

✉ sales@abusix.com | ☎ +1 (855) 522-8749 | 🌐 www.abusix.com