DATASHEET

Blacklist Monitoring.

Continuous IP and domain reputation monitoring across hundreds of blocklists, with an alert the moment a listing appears.

DOCUMENT	Product Datasheet
PRODUCT	Blacklist Monitoring
PUBLISHED	July 2026
SIGN UP	portal.generatorlabs.com/signup · first host free

Mail servers get blacklisted without sending a single spam message: a bad neighbor on a shared range, a compromised form, a policy listing, a list error. Nobody notifies you; your mail simply starts bouncing, and the first report usually comes from a customer who stopped receiving it. Blacklist Monitoring closes the gap: it watches your addresses against the blocklists receivers actually use, and tells you the moment anything changes.

01

Why Monitor

Spam share: Kaspersky Securelist, 2025. Inbox placement: Validity 2025 benchmark.

Roughly 45 percent of global email is spam, so receivers filter automatically and aggressively, checking blocklists at connection time before your message is ever read. Even clean, unlisted senders lose about 1 in 6 legitimate messages on the way to the inbox. A listing does not nudge those numbers; it cuts delivery to zero at every receiver that trusts the list, and it stays at zero until someone notices and starts the delisting process.

45%	1 in 6	0
OF ALL EMAIL IS SPAM	MISS THE INBOX	LISTS THAT NOTIFY YOU

02

What It Monitors

Source coverage is curated and kept current; a typical default scan checks 140+ blocklists per host.

`sources`	**Blocklists**	Hundreds of RBL and URIBL sources (including Spamhaus, Barracuda, SpamCop, SURBL, and URIBL), DNS security filters like Quad9, and threat exchanges like PhishTank and Project Honey Pot.
`hosts`	**Your Addresses**	Individual IPv4 and IPv6 addresses, domains, and whole IP ranges or CIDR blocks, so shared-range contamination is visible too.
`custom`	**Custom Sources**	Add your own RBLs, and control exactly which sources each monitoring profile checks and how often.

`manual`	**On-Demand Checks**	Run a manual check against every source at any time, on top of the scheduled monitoring cycle.

03

Notification channels include email, Slack, SMS, and webhooks, with contact groups and per-channel scheduling.

How It Works

1. Add Your Hosts	Register IPs, domains, and ranges in the portal or over the REST API.
2. We Check Continuously	Every host is checked against your selected sources on a schedule you control, around the clock.
3. You Get Alerted	The moment a listing appears, an alert goes out through your choice of more than a dozen channels, including email, Slack, SMS, and webhooks.
4. Resolve and Prove It	Every detection links to the blocklist's removal process, while listing history and shareable reports document your reputation over time.

Built for Automation

Everything in the portal is available over the REST API (v4): manage hosts, pull status, and wire alerts into your own tooling with webhooks. Monitoring fits into your stack instead of becoming one more dashboard you have to remember to check.

04

Platform figures as published at generatorlabs.com.

The Platform

30B+	10M+	500K+
CHECKS PERFORMED	CHECKS EVERY DAY	ACTIVE HOSTS

Blacklist Monitoring runs on the same Generator Labs platform as Certificate Monitoring, with shared contacts, alerting, and API access. Spot-check any address for free at mrdns.com/blacklist-check.

Your First Host Is Free

Add an IP or domain and Generator Labs Blacklist Monitoring will watch it against hundreds of blocklists around the clock. No credit card required.

portal.generatorlabs.com/signup